Xerox WorkCentre 5325/5330/5335 Information Assurance Disclosure Paper

Version 1.10, December 2011

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Table of Contents

Section 1 Introduction

1.1 Purpose

The purpose of this document is to disclose information for the Xerox WorkCentre 5325/5330/5335 products (hereinafter called as “the product”) with respect to device security. Device Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity, PDL’s, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1.2 Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Fuji Xerox be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Fuji Xerox has been advised of the possibility of such damages.

Section 2 Device Description

The product provides the copy and network printer functions and features, and consists of a controller module, marking engine and scanner.
In addition, the product also has an optional Fax kit, which adds a telephone modem and provides embedded Fax capabilities.

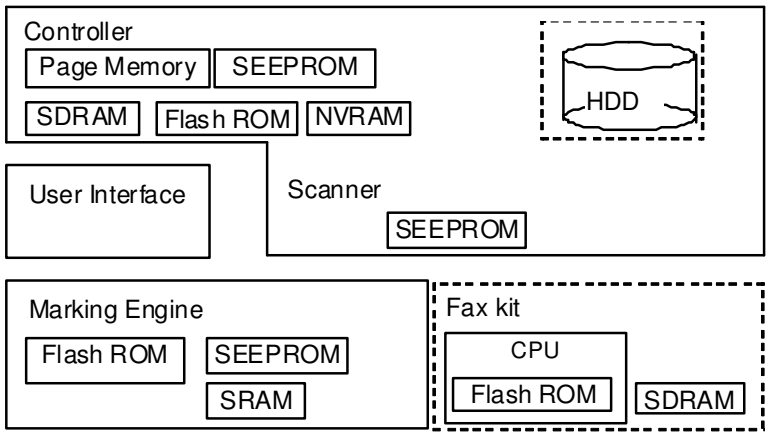
The following table lists the major elements of the product. CPS is Copier Printer Scanner.

Configuration	Marking Engine	Scanner	Controller	Fax Kit
CPS	X	X	X	

X: Included

2.1 Memory Devices of the Product

This section describes details of the memory devices that are contained within the product.
The memory devices are shown below:



2.1.1 User Interface

User image data in the memory on Controller is accessible by using Image View Kit (Preview Thumbnail feature).

2.1.2 Marking Engine

Name	Purpose/Explanation
Flash ROM	All operating system and application executable control code related to Marking Engine resides here (e.g. boot loader, paper path, and xerographic).
SRAM (Static RAM)	This is a Work RAM used to develop the program and parameters in the above-mentioned Flash ROM. No user data is stored in this memory.

2.1.3 Scanner

The scanner does not have its own control processor. The scanner attribute information is written in the SEEPROM and the control is performed by the controller.

Name	Purpose/Explanation
SEEPROM	This non-volatile memory has no user data stored in it. This memory contains: ・Mode setting information on image processing and mechatronics control, and data on the parts usage status associated with recycling.

2.1.4 Controller Memory Devices

The details of the memory devices in the Controller are:

Name	Purpose/Explanation
SDRAM	The executable software is loaded in this memory and is run. This memory is also used for temporary storage of user data such as data files and images. Such data is not backed up and is lost when the power to the product is removed.
Flash ROM	This Flash memory contains the code necessary to boot the system, all executable code (operating system, PostScript interpreter, network protocols, document scheduler, etc.), and the installed fonts. A power-on self-test is performed and the bootstrap OS is loaded. This memory never contains any user data or document data. Operating system and application executable control code resides here. All codes except for the code of boot loader is compressed and is extracted into DRAM to be executed. No user image data is stored in this memory.
NVRAM	This non-volatile memory has no image data stored in it. User data such as system setting information, mailbox information, speed dial information, job memory, user management information, and various types of logs are recorded in it. The data is written in the memory after it is encrypted.
Controller	This device contains numerous types of data including user data:

Hard disk	1) Data of the documents scanned in upon copying. 2) Data of spooled documents in PDL format from the network. 3) Data of the documents used in security print, sample print, and delayed- start print. 4) Data of the scanned-in documents 5) Data of the Fax-sent / Fax-received documents 6) Job logs. 7) Downloaded fonts and forms. For the formatting of the hard disk, the file system included in VxWorks is used. The format, however, is not accessible even when the hard disk is connected to PC. When a job is completed, its reference in the directory table is deleted but the image data remains on the disk until overwritten by a subsequent job. Image Overwrite feature enables an overwrite of the used data with meaningless data. Also, Data Encryption feature enables a data encryption.
Page Memory	This is a volatile memory used to store image data temporarily.
SEEP ROM	This memory contains the system's setting information.

2.1.5 Fax Kit

The Fax kit has its own control processor, and the Fax control software is executed from the Flash ROM.

Name	Purpose/Explanation
Flash ROM	This memory contains "Fax control software". No user data is stored in this memory.
SDRAM	This volatile memory stores "control data required to execute Fax control software" and "user data" temporarily.

2.1.6 Other Memory Devices

The product has other memory devices, but such devices are used solely as accessory devices that control I/O of paper. Examples of this distributed control are:

・Finisher, DADF, Duplex, and Tray Module

No user data is stored in any of these memory devices.

2.2 Operating Systems

The Marking Engines for the product contains the HI7000/4 operating system. These systems have no networking capability.

The Controller uses the VxWorks realtime operating system. Typical Unix functions such as Rsh, telnet and Finger do not operate under the OS.

User must note that the VxWorks operating system is not accessible. All logons to the product are to application software and not to the VxWorks OS. Hence the VxWorks OS is not accessible to the user.

2.3 Program Downloading

The programs stored in the Flash ROM listed below are downloadable from external sources.

- Controller
- Marking Engine
- Scanner
- Document Feeder
- Fax module (including added ports)
- Finisher (Option for processing printed paper. No description on Finisher is provided in this document because user's image data will not be stored in it.)
- High capacity feeder(No description on High capacity feeder is provided in this document because user's image data will not be stored in it.)

This program-downloading function can be disabled by a key operator from the local UI.

The header part of file is checked using software to identify whether the download file is legitimate.

Section 3 System Access

3.1 Physical Access

There are a variety of methods to physically access the system. To compromise the system, a person must be local to the device. Remote (logical) access is discussed in the next section.

3.1.1 User Interface

The User Interface is the control panel on the front of the device. From the UI, a user can:

- access to setup menus of Common, Copy, Print, Mail, Network, Fax, Mailbox, etc
- create his/her own Mailbox and Address Book
- access to setup menus of Auditron
- change the setting on Key Operator Tools

An ID and password required to enter Key Operator Tools mode are stored in the Controller NVM.

3.1.2 10/100/1000 MB Ethernet RJ-45 Network Connector

This is the standard network connector, and allows access to the connectivity stacks and open ports described in the next section. This connector conforms to IEEE Ethernet 802.3 standards.

3.1.2.1 Network Scan feature (1)

The product has a memory called Mailbox, to store the scanned-in data and the Fax/Internet Fax received data. Password can be assigned to Mailbox, and Mailbox is accessible only by a person who assigned the password and a person who is notified of the password; he/she can retrieve the image data in the Mailbox from the client PC via LAN. On the PC, installed Scanner Driver decodes the retrieved data to image.

3.1.2.2 Network Scan feature (2)

This is a feature to transfer the scanned-in data directly to the server on the LAN. The image data is directly converted into the specified format and sent.

Scanned-in image is generated by the device firmware. It is difficult to modify the firmware to add a virus. Also, since the Fax-received document is in the image stream received by the Fax protocol, it is difficult to implant a virus. Although image is received in TIFF file for Internet-Fax, since the received image is once converted into the internal format, image conversion error occurs if a virus is implanted in the image.

3.1.3 USB Port

USB2.0 port for maintenance

The USB2.0 port is the USB target connector provided to perform maintenance. This port is on the standard controller board; the firmware is downloaded using this port. The Fuji Xerox unique protocol is used for maintenance. From this port, software can be downloaded and diagnostics can be performed. No image data and document data is accessible through this port.

USB2.0 Port for printer

The USB2.0 port is the USB target connector used to print files via direct connection. The received data is processed by imaging software on the product.

USB2.0 Port (option)

The USB 2.0 port is used for Digital Camera Print with media reader connected, USB Memory Print / ScanToUSB with USB memory connected, and for connection with IC card reader. Note that this port may be disabled due to the status of the setting.

3.1.4 Accessory Interface

This port is used to connect optional equipment to control usage of the product. A typical application is a coin-operated device where a user must deposit money to enable the product to perform copying. The information available via the Accessory Interface is limited to information on copied sheets delivered to the finisher or output tray. No image job or document data is accessible through this port except for the counter data.

3.1.5 Fax Phone Line

The product does not provide a function to access the network via the Fax Phone Line.
Also on the Direct Fax *, the data passed from the client PC is only the compressed image data and destination information. Since any data other than image information (such as a virus, security code, and control code that directly access the network) is abandoned at this stage, such data is never sent from the network to Fax Phone Line.
* From the client PC that is connected to the LAN, normal print data with the destination number is sent to the product via the Ethernet. This print data is converted into image and encoded in Fax format, and sent to the Fax kit with the destination information.

Even when the product is accessed by a data communication equipment or the product accesses it, the product immediately ends the call without being connected properly, since the product can implement only Fax communication protocols but not data communication protocols. Thus, there is no mechanism to access the network via the telephone line.

Fuji Xerox certifies that it is not aware of any method by which a user can access the network via the Fax telephone line, which is connected to the product.

3.2 Logical Access

3.2.1 Network Protocols

The network protocols supported by the product are IP (IPv4/IPv6), BOOTP, DHCP, IPX, Apple Talk, SNMP（v1/v2c/v3）, NETBEUI/NETBIOS, SMTP, SSDP, SNTP, HTTP, Kerberos, LDAP, SLP v1, IPP, LPR, and so on. These protocol specifications are implemented based on standard specifications such as RFC issued by IETF.

3.2.2 Ports

A number of TCP/IP and UDP/IP ports exist. The following table summarizes all ports that can be opened, and subsequent sections discuss each port in detail for when the product uses them.

Port#	Type	Service name
20	TCP	FTP - Client -
21	TCP	FTP data - Client -
25	TCP	SMTP
53	TCP/UDP	DNS - Client -
67	UDP	BOOTP/DHCP - Client -
80	TCP	HTTP(CWIS)
80	TCP	HTTP(UPnP Discovery)
80	TCP	HTTP(WSD)
80	TCP	HTTP(WebDAV)
80	TCP	HTTP(IPP added port)
88	UDP	Kerberos - Client -
110	TCP	POP3 - Client -
123	UDP	SNTP - Client -
137	UDP	NETBIOS -Name Service
138	UDP	NETBIOS -Datagram Service
139	TCP	NETBIOS
161	UDP	SNMP
162	UDP	SNMP trap
389	TCP	LDAP - Client -
427	TCP/UDP	SLP
443	TCP	HTTPS(CWIS)
443	TCP	HTTPS(IPP)
443	TCP	HTTPS(WebDAV)

443	TCP	HTTPS(Authentication Agent)
445	TCP	Direct Hosting
465	TCP	SMTPS - Client -
500	UDP	ISAKMP
515	TCP	LPR
524	TCP	NetWare NCP - Client -
547	UDP	DHCPv6 - Client -
631	TCP	IPP
636	TCP	LDAPS - Client -
1824	TCP	HTTPS(OffBox Validation) - Client -
1824	TCP	Xerox Secure Access - Client-
1900	UDP	SSDP
5004 5005	UDP	Listener port for RTP communication
5353	UDP	mDNS
9100	TCP	raw IP
15000	TCP	Loopback port for the control of SMTP server
15010 15011	UDP	Loopback port for RTP communication control
20001	TCP	Loopback port for HTTP Server
1024-	TCP	NetWare, SLP

"- Client -": The port is not open on the controller all of the time but will open only at time of accessing the remote server.

3.2.2.1 Ports 20, 21: FTP

This port is not open all of the time. This port is open only when sending image data to the FTP server to perform ScanToFTP and MailboxToFTP functions, or when accessing the FTP server to search for Scan Job Flow Sheets (i.e. Scan job Flow Sheets). In other cases, no FTP connections are accepted on these or any other ports.

3.2.2.2 Port 25: SMTP

This port enables Internet Fax feature and E-mail Print feature, and is open all of the time when the receive protocol is set to SMTP. Also, this port is open when sending image or message to SMTP server in Internet Fax, Scan to E-mail, or Email Alert feature. When "SMTP Authentication" is set, authentication to the server is performed. In such case, a password is sent in plain text or as encrypted according to the information notified by the server. A key operator can change the port number from CentreWare Internet Services.

3.2.2.3 Port 53: DNS

This port is used for DNS. This port is used for name queries to the DNS server (stub resolver) when the product accesses the device designated by the device name. This port is also used to register device names in DNS server (authoritative server) to update the DNS dynamically. A key operator can disable only DNS dynamic update service from CentreWare Internet Services.

3.2.2.4 Port 67: DHCP

This port is used only when performing DHCP, and is not open all of the time. To permanently close this port, DHCP must be explicitly disabled. This is done via the Local User Interface or CentreWare Internet Services by a key operator.

3.2.2.5 Port 80: HTTP (CWIS)

This port is used to access embedded web pages through browser. The port number can be changed from CentreWare Internet Services by a key operator.
The embedded web pages are used for the following purposes:

- to give information on device status to users.
- to enable confirmation of the job logs and job queue in the device, and operation of the jobs.
- to allow users to download print ready files and program Scan Job Flow Sheets.
- to enable management of Mailboxes and operation on the documents in Mailboxes.
- to enable import/export of Address Book and import of device certificate.
- to allow remote administration of the device. User may view the properties but not change them without logging into the product with key operator privileges. When authentication of the key operator fails for the specified number of times consecutively, rebooting of the entire product is required.

A read/write of partial system setting information is possible through the unique protocols on the HTTP port.

The HTTP server can only host the web pages in the device, but cannot substitute for the proxy server. Through HTTP, the file system of the product cannot be accessed directly.

The embedded HTTP server is a product of Xerox.
A key operator can disable this service (and the port) via Local User Interface or from CentreWare Internet Services.

3.2.2.6 Port 80: HTTP (UPnP Discovery)

This port provides the discovery feature using SSDP. The port number is configurable, and a key operator can disable this service (and the port) via local UI or from CentreWare Internet Services.

3.2.2.7 Port 80: HTTP (SESAMi Manager)

The port number is configurable, and a key operator can change the port number via local UI, CentreWare Internet Services, or SSMI. Also, a key operator can disable this service via local UI, CentreWare Internet Services, or SSMI.
Port 80 operates as a HTTP server for SSMI. Port 443 operates as a secure channel for SSMI, and supports SSLv3 and TLSv1. When SSL is enabled, HTTP connections to SSMI are redirected to HTTPS. Since communication through port 443 is encrypted, interception on the network can be avoided.

3.2.2.8 Port 80: HTTP (WebDAV)

This port is a WebDAV server port that supports features to access Mailbox. The port number is configurable, and a key operator can disable this service (and the port) via local UI or from CentreWare Internet Services.

3.2.2.9 Port 88: Kerberos

The product employs Kerberos client function that is used to access this product from Local UI.
The product supports Kerberos V5 and uses CBC (Cipher Block Changing) of DES (Data Encryption Standard).
The Kerberos code is not used for document encryption.
The authentication data of the user permitted by the product is set in the Kerberos server, and address information and realm information of the Kerberos server used by the product is set in the Controller NVRAM.

The following show the difference from the standard Kerberos packaging.

1) Ticket cache
   In the product, tickets are stored only in a memory, and are deleted automatically by a user log-off or an automatic log-off due to time-out. When power is turned off during log-on, the tickets will be deleted.
2) Validity of the ticket
   In the product, only the initial ticket is obtained; authentication is considered as successful when the initial ticket is obtained. Thus, invalidation of the initial ticket is not judged.

3.2.2.10 Port 110: POP3

This port enables Internet Fax feature and E-mail Print feature, and is open at the specified intervals set when receive protocol is set to POP3. Also, when “POP Before SMTP” is set, POP access is always performed before sending data such as image to the SMTP server. Usually the POP User ID and the password are sent in plain text, but the password is encrypted to be sent when “APOP authentication” is selected.
A key operator can change the port number from CentreWare Internet Services.

3.2.2.11 Port 123: SNTP

This port is used to access the server at the specified intervals when time synchronization with the external time is set on the Local User Interface. The setting can be changed by a key operator.

3.2.2.12 Ports 137, 138, 139, 445: NETBIOS

Port 137 is the standard NetBIOS Name Service port and mainly used by WINS. Port 138 supports the CIFS browsing protocol. Port 139 is the standard NetBIOS Session port and is open all of the time for printing. Port 445 is a standard direct host port and is used for communication using SMB protocol that does not use NetBIOS over TCP. A key operator can disable each of the 4 ports via Local User Interface or from CentreWare Internet Services. To use the SMB feature for Scan, all of the above ports need to be available. For Scan, image is sent to Port 139 or Port 445, both of which are on the remote server.

3.2.2.13 Ports 161, 162: SNMP

These ports support the SNMPv1, SNMPv2c, and SNMPv3 protocols. SNMPv1 and SNMPv2 control access to device's MIB information by using write community string and read community string. Since these community strings are transmitted on network in plain text, users should note that the community strings can be read if packets are dumped. Fuji Xerox recommends that the customer changes the community string from the default upon product installation. To solve the above problem, for SNMPv3, packets on network are authenticated and encrypted, which realizes safe access. Therefore, users who place importance on security should use SNMPv3. A key operator can set enable/disable of the SNMP from the local UI or CentreWare Internet Services.

3.2.2.14 Port 389: LDAP

This is the standard LDAP port used for Address Book queries in LDAP authentication and the Scan to Email feature.

3.2.2.15 Port 427: SLP

In the product, this port is used to search the NetWare server on the network, on the IP protocol. This function operates only when the NetWare print function is set to be used on the IP protocol.

3.2.2.16 Port 443: HTTPS

This port operates as a secure channel for HTTP server, and supports SSLv3 and TLSv1. When SSL is enabled, HTTP connections to CentreWare Internet Services are redirected to HTTPS. Since communication through this port is encrypted, interception on the network can be avoided. A key operator can change the port number and/or disable the port via local UI or from CentreWare Internet Services.

3.2.2.17 Port 443: HTTPS (IPP)

This port operates as a secure channel for internet print protocol, and supports SSLv3 and TLSv1. Since communication through this port is encrypted, interception on the network can be avoided. A key operator can change the port number and/or disable the port via local UI or from CentreWare Internet Services.

3.2.2.18 Port 443: HTTPS (WebDAV)

This port operates as a secure channel for Web DAV server, and supports SSLv3 and TLSv1. When SSL is enabled, HTTP connections to WebDAV server are redirected to HTTPS. Since communication through this port is encrypted, interception on the network can be avoided. The port number is configurable, and a key operator can disable this service (and the port) via local UI or from CentreWare Internet Services.

3.2.2.19 Ports 80, 443: HTTPS (Authentication Agent ASC)

These are used as the destination ports when the product communicates to ApeosWare Authentication Agent (AWAA). Protocol and port number can be changed from AWAA by the system administrator (of AWAA) and cannot be changed from local UI or CentreWare Internet Services.

3.2.2.20 Port 465, SMTPS

This is the secure channel port used to access the SMTP server using SMTPS (SMTP over SSL) for Scan to Email, Internet Fax Send, and Email Alert.

3.2.2.21 Port 500: ISAKMP

This port is used for IKE in order to establish an IPSec SA (Security Association), and is open all of the time for IKE communication. When the product communicates to an external device as a client, the port number of the product and that of the external device are both 500. A key operator can disable IPSec via local UI or from CentreWare Internet Services.

3.2.2.22 Port 515: LPR

This is the standard LPR printing port, which only supports IP printing. The port number is configurable and a key operator can disable this service (and the port) via Local User Interface or from CentreWare Internet Services.

3.2.2.23 Port 524: NetWare NCP

This is a port on the NetWare server side, and is used to provide print service through IP connection to NetWare server. After connection, the port is used until the power is turned off. The port number cannot be changed. A key operator can disable the service via local UI or from CentreWare Internet Services.

3.2.2.24 Ports 546, 547: DHCPv6

These ports are used for DHCPv6. When querying the IPv6 DNS server address, the product accesses port 547 of DHCPv6 server and receives the result from DHCPv6 server at port 546. The product can query the IPv6 DNS server address when the auto acquisition of IPv6 DNS server address is enabled, and a key operator can disable it from CentreWare Internet Services.

3.2.2.25 Ports 80, 631: IPP

These ports support the Internet Print protocols. 631 is the standard port number for IPP and 80 is an added port number. The added port number is configurable. A key operator can disable this service (and the ports) via Local User Interface or from CentreWare Internet Services.

3.2.2.26 Port 636: LDAPS

This is the secure channel port used to access LDAP server using LDAPS (LDAP over SSL) for LDAP authentication and for Address Book queries in the Scan to Email feature.

3.2.2.27 Port 1824: HTTPS (OffBox Validation)

This port is used to communicate with OffBox Validation server. The protocol and port number can be changed by the system administrator on the OffBox Validation server side and cannot be changed via local UI or from CentreWare Internet Services.

3.2.2.28 Port 1900: SSDP

This port provides the discovery feature that complies with SSDP (Simple Service Discovery Protocol). This port number cannot be changed. Whether this port opens depends on whether the UPnP discovery feature is/are enabled or disabled.

3.2.2.29 Port 5353: mDNS

This port provides the discovery feature using Multicast DNS. The port number is fixed to 5353. A key operator can disable this service via local UI or from CentreWare Internet Services.

3.2.2.30 Port 9100: raw IP

This port has a bidirectional function (via pjl back channel), and only allows printing. The port is a configurable port and a key operator can disable this service (and the port) via Local User Interface or from CentreWare Internet Services.

3.2.2.31 Port 15000: Loopback Port

This port is the loopback port for the control of the common server that operates the SMTP server, and is activated when SMTP receive is enabled. A key operator can disable this loopback port by disabling SMTP receive via Local User Interface or from CentreWare Internet Services.

3.2.2.32 Port 5004/5005: Listener Port for RTP Communication

This port is the listener port for RTP communication and is used in combination with the RTP (port 5004), which is the real time transport protocol, and the RTCP (port 5005), which controls the RTP session. The former port is activated to standby for Fax signals when incoming call occurs for IP Fax. A key operator can change the port number via Local User Interface or from CentreWare Internet Services.

3.3 Log-in and Authentication Methods

The product provides a number of authentication methods for different types of users. In addition, the product also logs into remote servers according to the features to use. Details of the operations follow.

3.3.1 Administrator Authentication

The following authentication information is stored in the product NVM. At the shipment, a default password is set. Xerox strongly recommends that this password is changed from the default value immediately upon product installation.

3.3.1.1 Local Access

To access the product from the local User Interface, a User ID and password of 4 to 12 letters are required. It is possible to set the product to be accessed using 1 to 32-byte user password.

3.3.1.2 Remote Access

To access the product from Xerox software products, a User ID and password of 4 to 12 letters are required. The password is used to access Administration screens on the Xerox software products.

3.3.2 Service Technicians Authentication

Authentication is also required for Xerox Service Technicians.

3.3.2.1 Local Access

To access the product from the local User Interface, a password is required. The key operator can restrict Service Technicians authentication.

3.3.2.2 Remote Access

There is not a way to access the product as a Service Technician from remote such as from the network.

3.3.3 General Users Authentication

The product provides the authentication function for general users.

3.3.3.1 Local Access

To access the product from the Local User Interface, authentication is required per the authentication method as shown below.

Authentication Method	Operation
No authentication	No authentication is required for general users.
Authentication on the product (without password)	When Authentication on the product is in enabled state, the User ID (PIN) is required for general users.
Authentication on the product (with password)	When Authentication on the product is in enabled state, the User ID and 4 to 12 digit password are required for general users.
Card Auditron	General user is required to insert the authentication card.
External authentication	When external authentication is in enabled state, general users access external authentication function for local access such as for copy / scan / Fax-send. The following are the external authentication functions, and input of the User ID and password is required. 1) Kerberos authentication 2) SMB authentication 3) LDAP authentication Description of each authentication function follows.

3.3.3.1.1 Kerberos Authentication

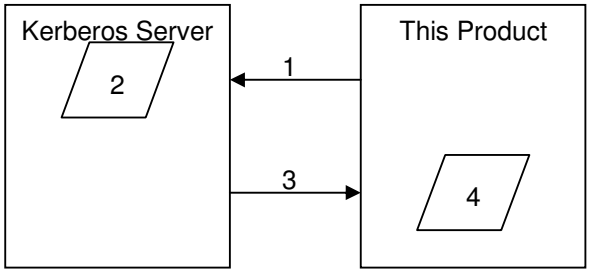
Kerberos authentication can avoid password interception and replay attack by using Kerberos protocol. The authentication steps using Kerberos are:

(1) A user enters the User ID and password from the Local User Interface on the product. The product encrypts the entered User ID and time stamp into authentication identifier using the password, and sends the authentication identifier to the Kerberos server.

(2) The Kerberos server decrypts the authentication identifier using the stored user password, to authenticate and obtain the included time stamp. Then, the server checks the validity of the time stamp. When the time stamp is correct, the Kerberos server creates a Session Key and encrypts it using the user password.

(3) The Kerberos server sends back the Initial Ticket that includes the encrypted Session Key to the product.

(4) The product decrypts the Session Key included in the Initial Ticket that the product received, using the entered password. When the decryption completes in success, the user is authenticated.



3.3.3.1.2 SMB Authentication

In SMB authentication, through the negotiation with SMB authentication server, the appropriate authentication method is determined by examining from the highest level (i.e. NVLMv2). User selects pre-registered SMB domain name, and executes authentication by entering User ID and password.

SMB Authentication Method	Operation
NTLMv2 authentication	This is supported by Windows OS of WinME/WinNT-SP4/2000/XP/2003. By challenge/response, authentication is executed without sending password directly to network. The authentication level is higher than NTLMv1 authentication.
NTLMv1 authentication	This is supported by Windows OS of WinNT/2000/XP/2003. By challenge/response, authentication is executed without sending password directly to network.
LM authentication	This is the authentication method adopted on LAN Manager. This is supported by Windows OS of Win95 and later. By challenge/response, authentication is executed without sending password directly to network. This is more vulnerable than NVLMv1 authentication.
PLAIN authentication	This is an authentication using plain text.

3.3.3.1.3 LDAP Authentication

The following modes are supported as the authentication methods in LDAP authentication. Since authentication on LDAP server is executed through Simple Bind using plain text, there is a risk of interception of User ID and password on network when LDAP protocol (port 389) is used. When LDAP server supports LDAPS protocol that uses secure channel using SSL, interception of User ID and password on network can be avoided by using LDAPS.

LDAP Authentication Mode	Operation
Direct Login	Executes authentication (ldap_bind) on LDAP server using User ID and password entered by user on local UI.
Search & Login	Searches user's Login ID from LDAP server using the User ID entered by user on local UI as a specific attribute (such as ID number), and executes authentication (ldap_bind) on LDAP server using the searched user's Login ID and entered password.

3.3.3.1.4 Secure Access Authentication

In Secure Access Authentication, since a secure channel communication using Secure Access Authentication server and SSL is performed, interception of User ID and password on network can be avoided. Communication between Secure Access card reader and Secure Access Authentication server is encrypted by the supplier's unique code.

Sequence of authentication performed by inserting card to Secure Access card reader is as follows:

1) The information on the card inserted to Secure Access card reader is read and notified to the Secure Access authentication server. Then, the request for password confirmation is notified to the product from the Secure Access authentication server. When the User ID is entered from the local UI, the User ID is notified to the Secure Access authentication server from the product, and the request for password confirmation is notified to the product from the Secure Access authentication server.
2) The product sends the entered password to the Secure Access Authentication server, and the Secure Access Authentication server sends back the validation result to the product.

3.3.3.2 Remote Access

To access various features on the product from the remote, authentication is required as follows:

Feature	Operation
Mailbox	To access the Mailbox from the Scanner Driver / CentreWare Internet Services, Mailbox number and password are required.
CentreWare Internet Services	With "Authentication on the product (with password)" selected, the User ID and password are required even to access the product from the browser.
Print Auditron	With the Print Auditron enabled, the User ID and password are required to be set on the Printer Driver.

3.3.4 Login to External Servers

To use the following features, the product logs into the external servers.

Feature to use	Operations of the product
ScanToMail / Internet Fax send / MailboxToMail / MailboxToInternet Fax	To use this feature, the product accesses the SMTP server set to the product. The following authentication methods are supported: *SMTP authentication (AUTH-PLAIN / AUTH-LOGIN / AUTH-CRAM-MD5/GSSAPI) *POP before SMTP (basic authentication / APOP) Also, to use the remote Address Book in this feature, the product accesses the LDAP server set on the product. In this case, a bind by SIMPLE authentication will be conducted, using the User ID and password set on the product.
ScanToFTP / MailboxToFTP	To use this feature, the product accesses the FTP server registered in the Address Book. The following authentication method is supported: * basic authentication
ScanToSMB / MailboxToSMB	To use this feature, the product accesses the SMB domain server registered in the Address Book. The following authentication methods are supported. For the authentication method, the product automatically selects the most powerful method through the negotiation with the server. * GSSAPI * LM authentication * NTLMv1/v2
Mail / Internet Fax receive (POP3)	To use this feature, when the receive protocol is set to POP3, the product accesses the POP3 server set on the product. The following authentication methods are supported: * basic authentication * APOP
Netware Print Server	The product accesses the NDS server using the User ID and password set on the product, in order to operate in NDS Printer Server mode.
IP Fax (SIP)	To use this feature when the setting is set to use the SIP server, the product accesses the SIP server set on the product. The following authentication method is supported: * Digest authentication

3.3.5 Single Sign On (SSO)

SSO is a feature that enables a user who has already logged into the device to access the external server without performing authentication again. The authenticated user's user ID and password are used to access the external server. SSO is available in the following services when the authentication method is external authentication.

Service	Operation Description
Remote Address Book	Authenticated user's user ID and password that were used for external authentication are used for authentication to access the LDAP server. When the external authentication method is Kerberos, the product obtains a service ticket and accesses the LDAP server using SASL protocol.
ScanToMail	Authenticated user's user ID and password that were used for external authentication are used for authentication to access the SMTP server. When the remote authentication method is Kerberos, the product obtains a service ticket and accesses the SMTP server.
ScanToHome	Authenticated user's user ID and password that were used for external authentication are used for authentication to access the server. When the remote authentication method is Kerberos and the product transfers the scanned information to the SMB server, it obtains a service ticket and accesses the SMB server.
ScanToPC	Authenticated user's user ID and password that were used for external authentication are used for authentication to access the server. When the remote authentication method is Kerberos and the product transfers the scanned information to the SMB server, it obtains a service ticket and accesses the SMB server.
CenterWare ScanServices	Authenticated user's user ID and password that were used for external authentication are used when the Login Source described in Job Template is "UserLogin / DomainUser / PromptIfNecessary." When the remote authentication method is Kerberos and the product performs ScanToHTTP, it obtains a service ticket and accesses the HTTP server.

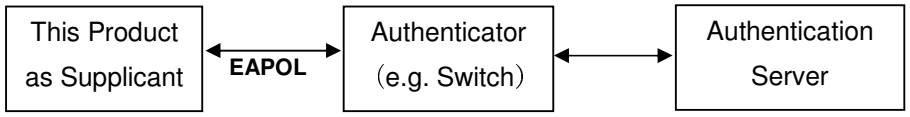
3.4 Device Authentication Method

The product provides the device authentication feature that is required for network connection to LAN port where access is controlled.
The following device authentication method is provided.

Device Authentication Method	Operation
802.1X	Wired 802.1X authentication is supported. When the product is activated using the User ID and password set for the product, authentication to the switch device starts in order to connect to the LAN port.

3.4.1 802.1X Authentication

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch as shown below, the Authentication server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result.
The product starts authentication processing at startup when the startup settings for 802.1X authentication is enabled.



Of the authentication methods in 802.1X Authentication, the product supports the following.

802.1X Authentication Method	Operation
MD5	Performs authentication using the ID information in plain text and MD5 hashed password.
MS-CHAPv2	Performs authentication using the ID information in plain text and MD5 hashed password that is encrypted using a key generated from random numbers.
PEAP/MS-CHAPv2	Performs authentication in the SSL-encrypted channel established between the product and the Authentication server, using the following information: - ID information in plain text. - Password encrypted in MN-CHAPv2 method.

3.5 FIPS140

FIPS140 are series of publications which are U.S. government security standards that specify requirements for cryptography modules.
The following operation modes can be selected.

Operation Mode	Description
FIPS140 approved Mode	In this mode, the algorithms that are specified in FIPS and are recommended by NIST are used in accordance with the requirements for FIPS140-2.
FIPS140 non-approved mode	The algorithms that are specified in FIPS and/or are recommended by NIST, and other algorithms operate in this mode.

The following are the approved algorithms that operate in FIPS140 approved Mode.

Algorithm approved by FIPS140
AES
3DES
DH
DSA
FIPS 186-2 PRNG
RSA X9.31, PKCS#1 V.1.5
RSA
SHA-1
HMAC-SHA1

Although SMB, NetWare, SNMPv3, and PDF Direct Print Service use encryption algorithms that are not approved by FIPS140, they can operate in FIPS140 approved Mode in order to maintain compatibility with conventional products.

Section 4 Data Flow

4.1 Print Service

4.1.1 Direct Print

Direct print is to print by outputting data to the printer ”without using the HDD” after decomposition of the received PDL.

<Condition>

This is a mode used at printing a single copy, or at printing multiple sets of copies without collating.

<Operation>

(1) Stores the received PDL in the spool area.

* In non-spool mode, PDL is not spooled and the ring buffer is overwritten.

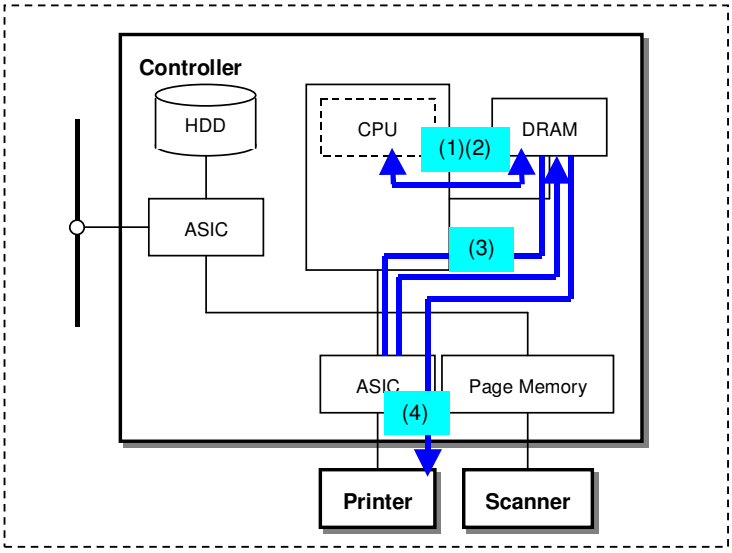
(2) Reads out the PDL stored in the spool area.

(3) Decomposes the read-out PDL per page, and writes in the page buffer (DRAM).

(4) Compresses the image per page, and outputs the compressed image for the page read out from the DRAM to the printer through decompression when compression for one page is completed.

(5) Deletes the received PDL data when printing of all data is completed.

* In spool mode only.



4.1.2 EPC Print

EPC Print is to print by outputting data to the printer "using the HDD" after decomposition of the received PDL.

<Operation>

Step1

(1) Stores the received PDL in the spool area (DRAM or HDD).

* In non-spool mode, PDL is not spooled and the ring buffer is overwritten.

(2) Reads out the PDL stored in the spool area.

(3) Decomposes the read-out PDL per page, and writes in the page buffer (DRAM).

(4) Compresses the page buffer per page and transfers to the DRAM.

(5) Reads out the compressed data from the DRAM, then transfers and stores it in the HDD.
Deletes the information in the page buffer after page image is transferred to the HDD.

Step2

(6) Reads out the compressed image from the HDD and transfers to the DRAM.

(7) Outputs the compressed image read out from the DRAM to the printer through decompression.

(8) Deletes the received PDL data when printing of all data is completed.

* In spool mode only.

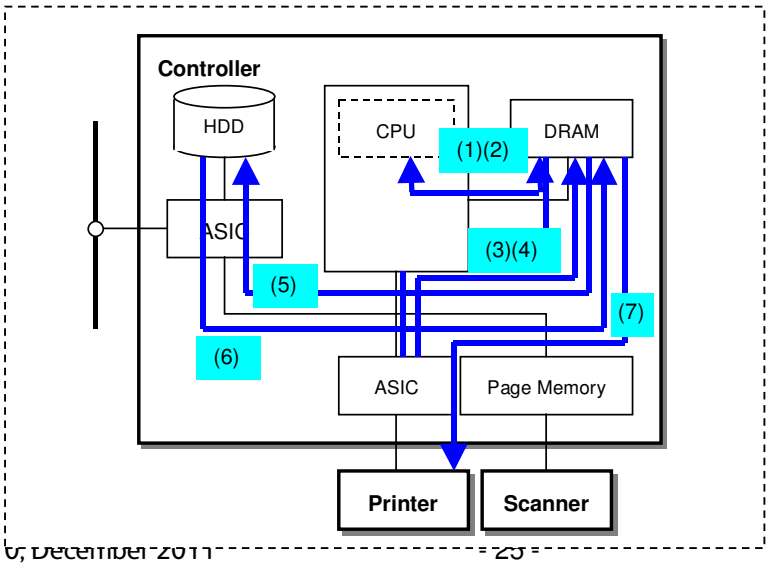
Password in Security Print

In the case of security print, the user ID and password is included in the received PDL and stored in the HDD with the page image.

When printing, the user ID and password input from the control panel is compared with that stored in the HDD. Printing is conducted only when the two matches.

Deletes the user ID and password recorded in the HDD when printing for all data is completed.

* User can set the product to keep the user ID and password in the HDD even after printing is completed.



4.1.3 Media Print / USB Memory Print

Media Print / USB Memory Print are to print by outputting data to the printer after decomposing digital camera data (EXIF) and/or document files (PDF, TIFF, etc.) stored in any media or USB memory.

<Operation>

Step1

(1) Reads out the data stored in any media or USB memory.

(2) Decomposes the read-out data per page and writes them in the page buffer (DRAM).

The processing after writing in the page buffer is the same as that in Direct Print and EPC Print.

4.2 Copy Service

4.2.1 Direct Copy Job

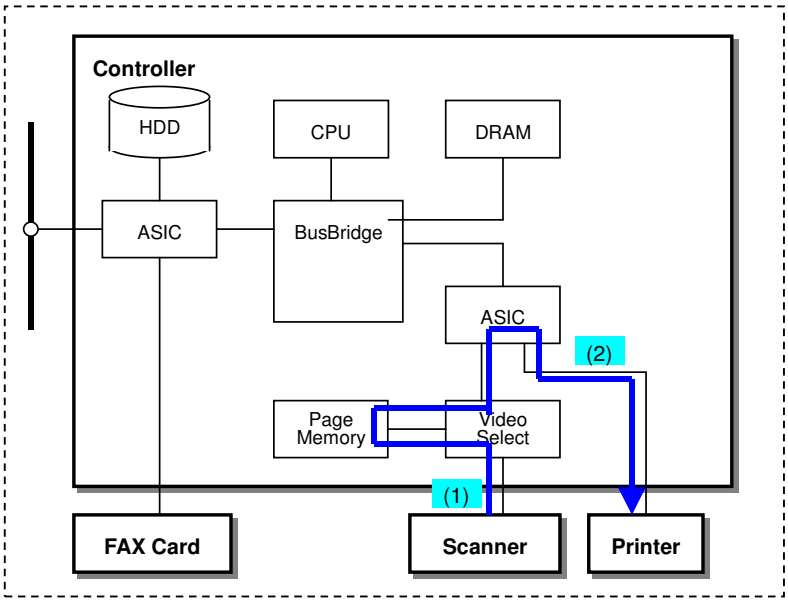
Direct copy job is to copy by outputting image data scanned by the scanner to the printer without compression and "without using the DRAM." (Used when reading data from the platen etc.)

<Operation>

(1) Stores the image data scanned by the scanner in the page memory.

(2) Outputs the image data read out from the page memory to the printer without compression, and by passing through Codec.

(3) Deletes the content of the page memory per page, every time the output of a page to the printer is completed.



4.2.2 EPC Copy Job (1)

This is to copy by outputting image data scanned by the scanner to the printer "using the HDD or DRAM." Image data is always stored in the HDD or DRAM, read out from the HDD or DRAM, then output to the printer. Accordingly, all the outputs to the printer for the first set and the subsequent sets are made after data is read out from the HDD or DRAM.

<Operation>

When printing is performed during scanning, Step1 and Step2 are executed concurrently.

Step1

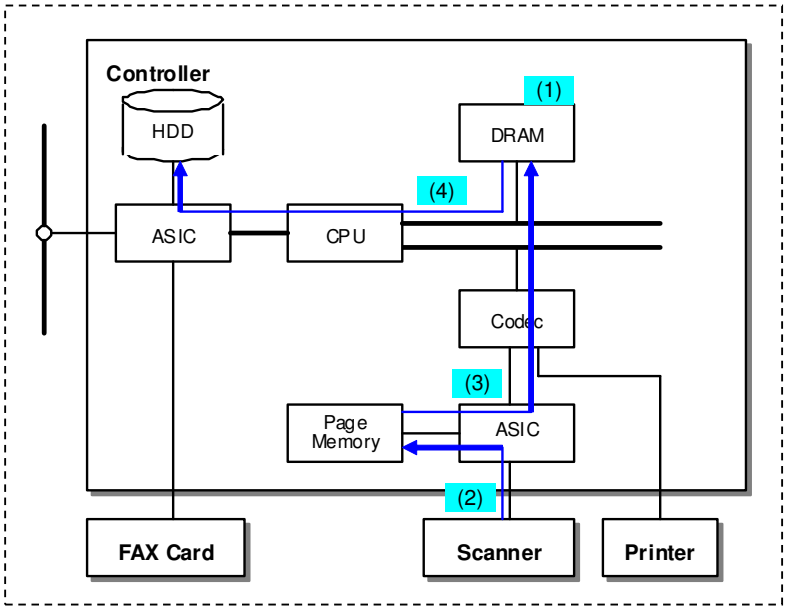
(1) Reserves area of the size for a single page in the DRAM as available memory.

(2) Stores the image data scanned by the scanner in the page memory.

(3) Compresses the image data read out from the page memory with Codec and transfers to the DRAM. Deletes the content of the page memory after data is read out from the page memory.

(4) Reads out the image data from the DRAM and stores in the HDD, after transferring of the image data to the DRAM is completed.
Deletes the content of the DRAM after image data is stored in the HDD. (4) is performed only when HDD is used.

Conducts the operations (2) to (4) for the number of times that equals to the number of pages scanned.



Step2

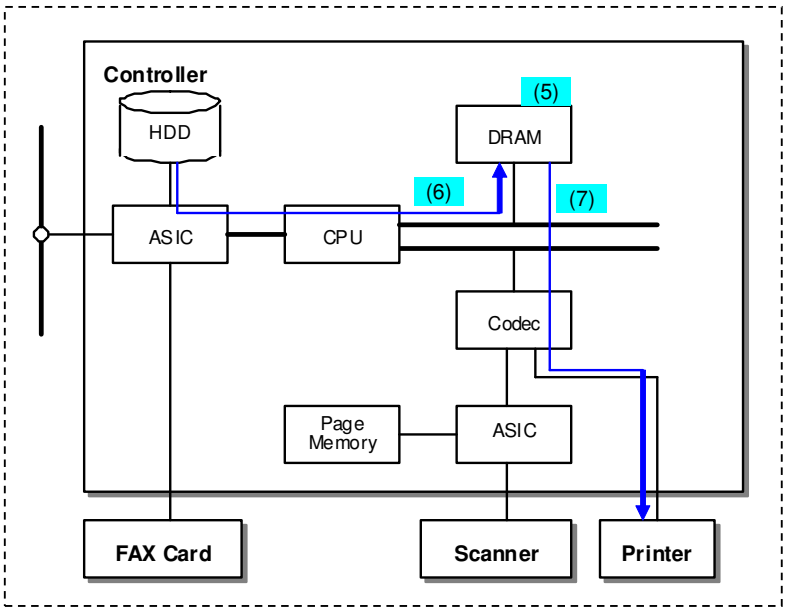
(5) Reserves printing area of the size for a single page as available memory in the DRAM.

(6) Reads out the compressed image from the HDD, and transfers the image for a single page to the DRAM. (6) is performed only when HDD is used.

(7) Outputs the data to the printer through decompression with Codec, after transferring of the data to the DRAM is completed.

Conducts the operations (6) to (7) according to the number of pages and sets.

(8) Deletes the images in the HDD after all images are printed. (8) is performed only when HDD is used.



4.2.3 EPC Copy Job (2)

This is to copy by transferring the image data scanned by the scanner to the DRAM, outputting the data to the printer from the DRAM, and also storing the data in the HDD.

<Operation>

Step1

(1) Reserves area for a single page in the DRAM as available memory.

(2) Stores the image data scanned by the scanner in the page memory.

(3) Compresses the image data read out from the page memory with Codec and transfers to the DRAM. Deletes the content of the page memory after data is read out from the page memory.

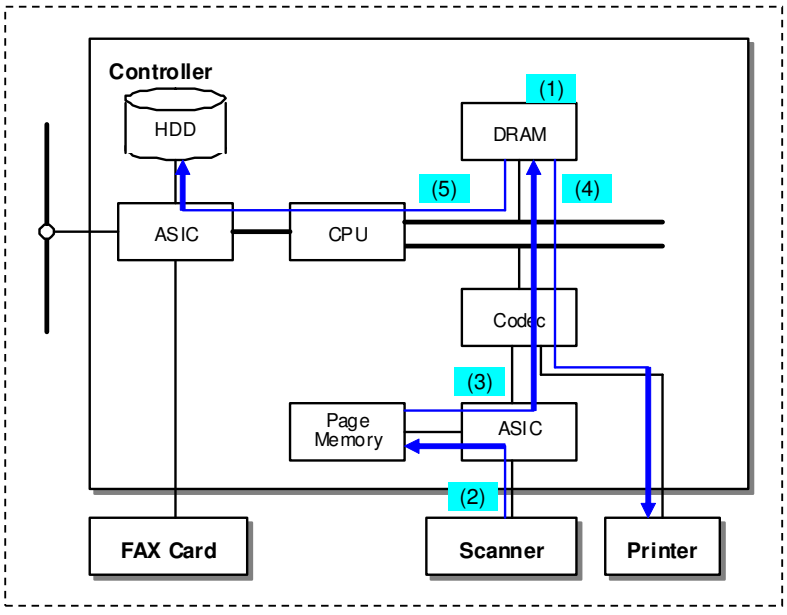
(4) Outputs the compressed image read out from the DRAM to the printer through decompression with Codec, after transferring of all the images for a single page to the DRAM is completed.

(5) Reads out the data from the DRAM and stores in the HDD, along with operations in (4).Deletes the page image in the DRAM after storing of the data in the HDD is completed.

Conducts the operations (2) to (5) for the number of times that equals to the number of pages scanned.

Step2

Executes the same operation as Step2 in "4.2.2 EPC Copy Job (1)"



4.3 Fax Service

4.3.1 Storage of Scanned Image

This is to scan image from the scanner, execute image processing as required, and then store in the HDD.

<Operation>

(1) Stores the image data scanned by the scanner in the page memory.

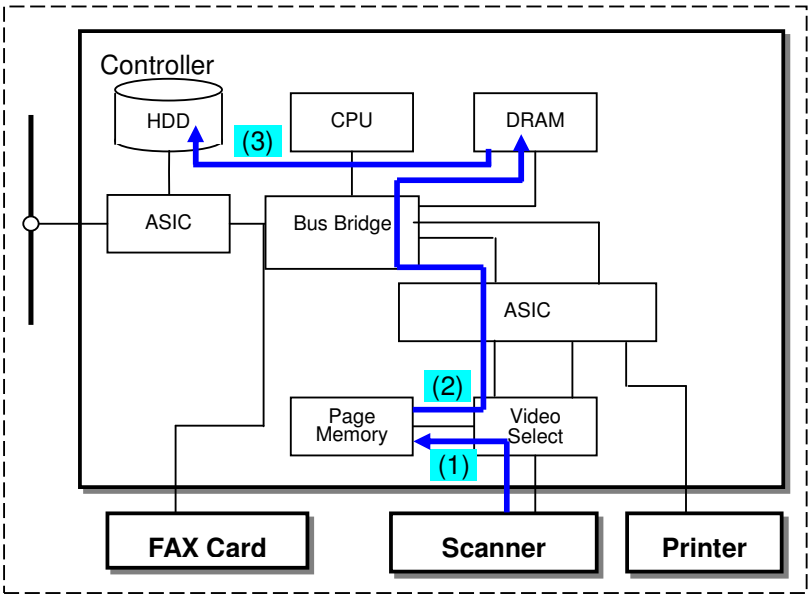
(2) Transfers the image data for one page read out from the page memory to the DRAM through compression.

Deletes the content of the page memory after transferring of the image data is completed.

(3) Stores the compressed data for one page read out from the DRAM to the HDD.

Deletes the page image in the DRAM and Fax Card after storing the compressed data in the HDD.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.



4.3.2 Fax Send

In Fax send, image data stored in the HDD is read out and output to the Fax Card.

<Operation>

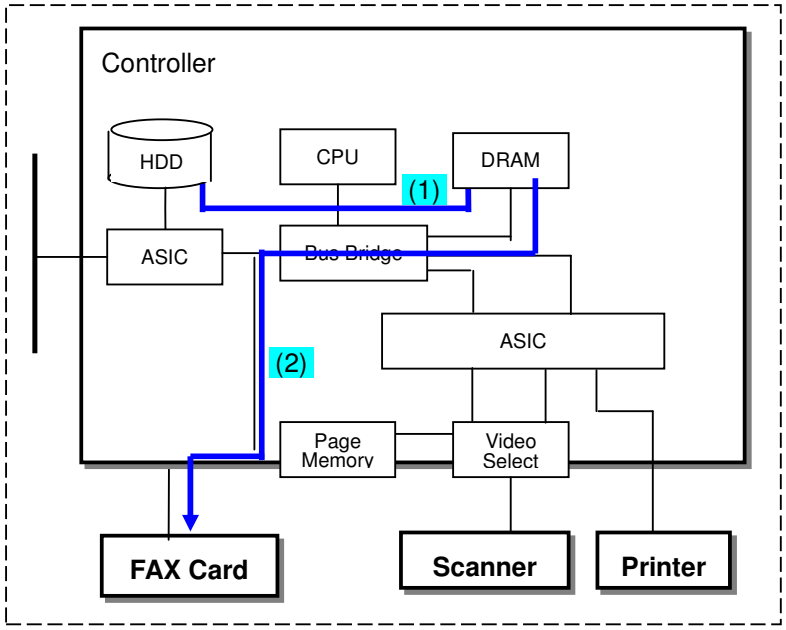
(1) Reads out the image data from the HDD and transfers to the DRAM

(2) Transfers the source information generated in the CPU and the image data read out from the DRAM to the Fax Card.

(3) Deletes the page image in the Fax Card every time a page of the document is sent.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.

(4) Deletes the document image in the HDD when all pages are sent completely.



4.3.3 Fax Receive

In Fax receive, image data received by the Fax Card is stored in the HDD.

<Operation>

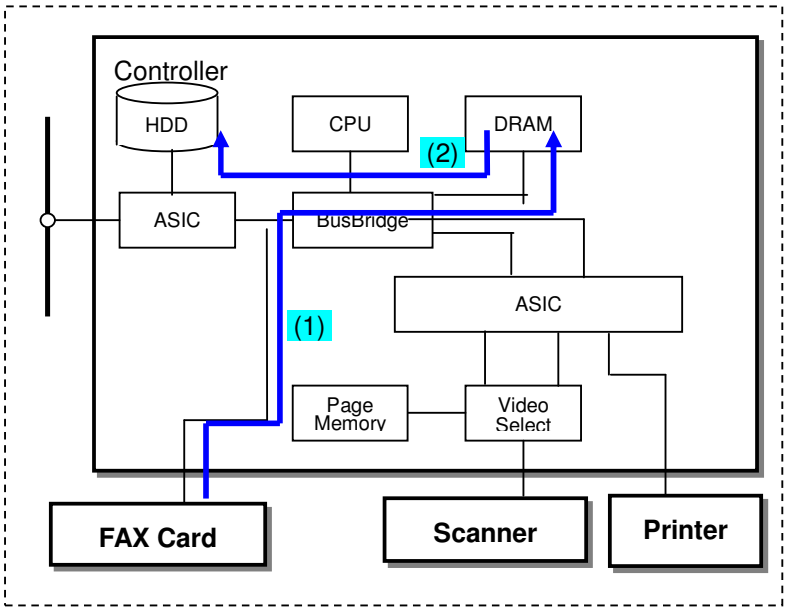
(1) Reads out the image data from the Fax Card and transfers directly to the DRAM.

(2) Transfers the image data read out from the DRAM directly to the HDD.

Deletes the page image in the DRAM after data is transferred to the HDD.

Conducts the operations (1) to (2) for the number of times that equals to the number of pages received.

At the time of receiving data, user can set the product to communicate only with a specific terminal by comparing the information that identifies the caller and the information of the terminal notified on the protocol etc.



4.3.4 Fax Print

In Fax print, image data received by the Fax Card is read out from the HDD. After decompression, image processing (rotation), and compression of the data is performed, the image data is stored in the HDD. Then, the image data stored in the HDD is output to the printer.

<Operation>

Step1

(1) Reads out the image data from the HDD and transfers to the DRAM.

(2) Decompresses the image data of DRAM and restores it in the DRAM.

(3) Converts resolution, merges or divides the page, and/or rotates the image read out from the DRAM as required, then restores the data in the DRAM.

(4) Compresses the image data read out from the DRAM and restores in the DRAM.

(5) Stores the image data in the HDD. Deletes the page image in the DRAM and the image data in the Fax Card.

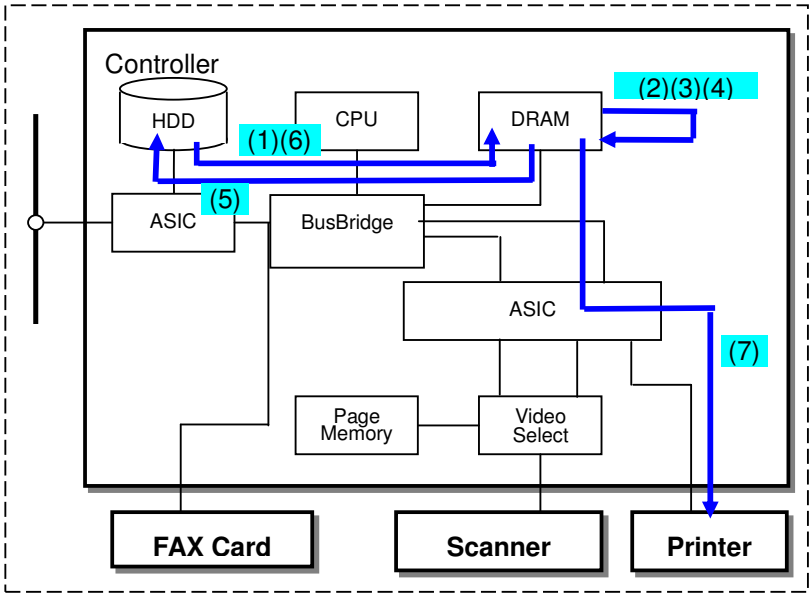
Conducts the operations (1) to (5) for the number of times that equals to the number of pages stored.

Step2

(6) Reads out the compressed image from the HDD and transfers to the DRAM.

(7) Outputs the compressed image read out from the DRAM to the printer while performing decompression.

(8) Deletes the page image in the DRAM and document image in the HDD after all the pages are printed.



4.3.5 IP Fax (SIP) Send

In IP Fax Send, image data stored in the HDD is sent via the Ethernet after the resolution is converted and compression is performed.

<Operation>

* Operations of storing the image data scanned from the Scanner to the HDD is the same as described in section "4.3.1 Storage of Scanned Image."

(1) Reads out the image data from the HDD and stores it in the DRAM.

(2) Reads out the image data from the DRAM, decompresses the data at the ASIC, and stores the data in the DRAM.

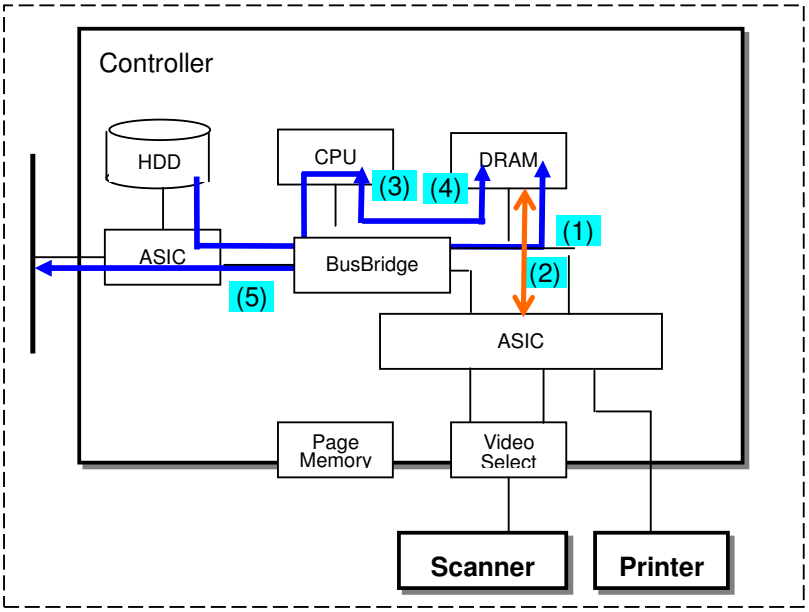
(3) Reads out the uncompressed image data from the DRAM, performs reduction and converts resolution at the CPU, and stores it in the DRAM.

(4) Reads out the uncompressed image data from the DRAM, creates transmission header text and merges it with the image data at the CPU, and stores the merged image data in the DRAM.

(5) Reads out the uncompressed image data from the DRAM, performs compression (JIBG/MH/MR/MMR) at the CPU, and sends it via the Ethernet.

Repeats the operations (1) to (5) above per page until all the pages are sent.

(6) Deletes the document image in the HDD after all pages are sent.



4.3.6 IP Fax (SIP) Receive

In IP Fax Receive, the received image data is stored in the HDD after compression is performed.

<Operation>

(1) Reads out the image data (JBIG/MH/MR/MMR) received via the Ethernet and stores it in the DRAM.

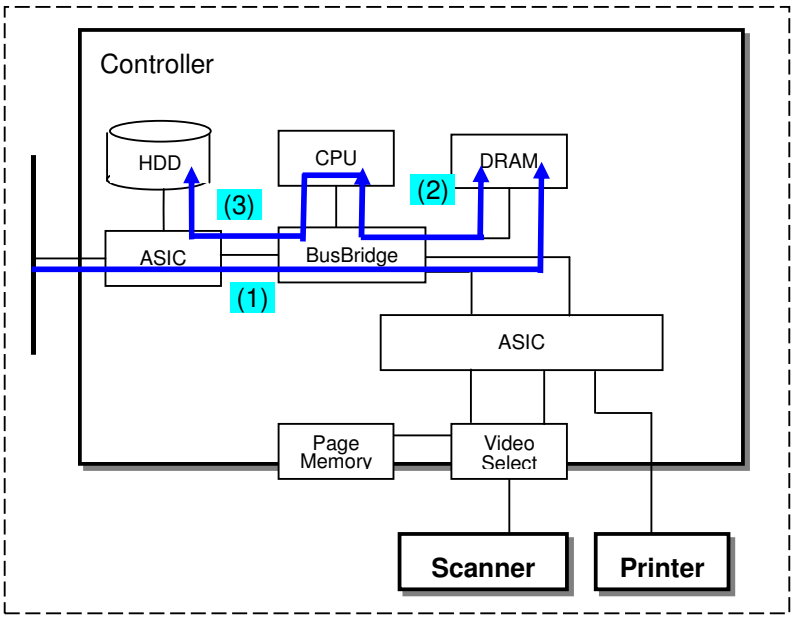
(2) Reads out the image data from the DRAM, decompresses the data at the CPU, and stores it in the DRAM.

(3) Reads out the uncompressed image data from the DRAM, performs JBIG compression at the CPU, and stores it in the HDD.

(4) Deletes all the page images in the DRAM after they are transferred to the HDD.

Repeats the operations (1) to (4) for the number of times that equals to the number of pages stored.

* Operations of outputting the image data stored in the HDD to the Printer is the same as described in section "4.3.4 Fax Print."



4.4 Direct Fax Service

In direct Fax service, the received PDL is decomposed and the compressed image is stored in the HDD, then parameters concerning send are output to the Fax Card.

<Operation>

Step1

(1) Stores the received PDL in the spool area (DRAM).

(2) Reads out the PDL stored in the spool area.

(3) Decomposes the read out PDL and writes in the page buffer (DRAM).

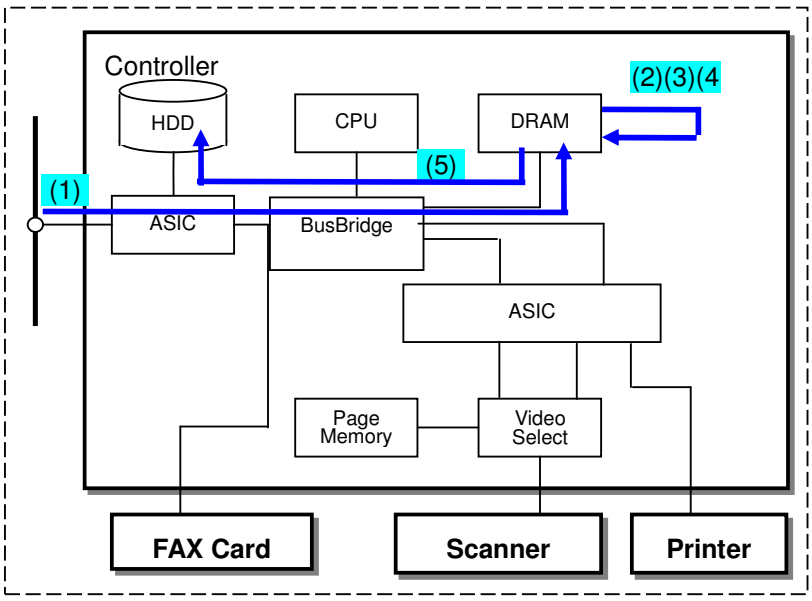
(4) Compresses the page buffer by each page and transfers to the memory.

(5) Reads out the compressed image data from the DRAM, then transfers and stores in the HDD.

Deletes the received PDL information and page buffer information after transferring of the page image to the HDD is completed.

Step2

See "4.3.2 Fax Send."



4.5 Scan Service

4.5.1 Scan to PC Service

In scan to PC service, the image data scanned by the scanner is converted into multipurpose image format (TIFF/JFIF/XDW/PDF/XPS) and transferred to the external device. When the machine designates transferring of the data to an external device via network, the data is transferred using the designated protocol (FTP, SMTP, or SMB).
According to the multipurpose image format, the following security feature can be used.

Format	Operation
PDF	Encryption using password: encrypts PDF document using password. Generated PDF document can be opened only by entering the same password. PKI signature: provides signature on PDF document using the device's digital certificate. Falsification and alteration of the generated PDF document can be detected and prevented if such changes are made on the document at the outside of the device.
DocuWorks	Encryption using password: encrypts DocuWorks document using password. Generated DocuWorks document can be opened only by entering the same password. PKI encryption: encrypts DocuWorks document using the receiver's public key certificate. The generated document can be opened only by presenting the private key certificate. PKI signature: provides signature on DocuWorks document using the device's digital certificate. Falsification and alteration of the generated DocuWorks document can be detected and prevented if such changes are made on the document at the outside of the device.
XPS	PKI signature: provides signature on XPS document using the device's digital certificate. Falsification and alteration of the generated XPS document can be detected and prevented if such changes are made on the document at the outside of the device.

<Operation>

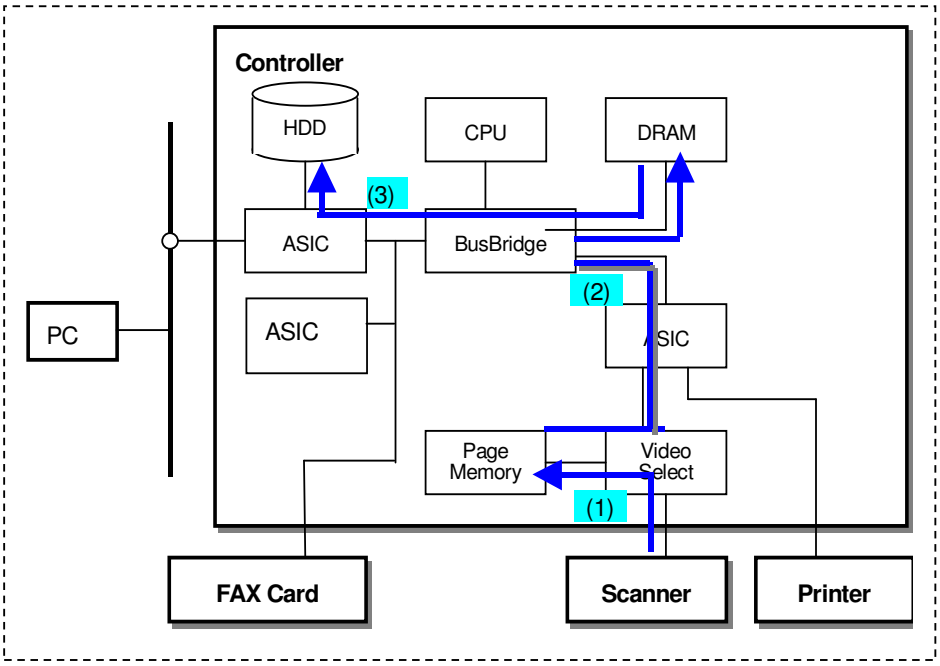
Step1

(1) Stores the image data scanned by the scanner in the page memory.

(2) Transfers the image data for one page read out from the page memory to the DRAM after compression.
Deletes the image in the page memory after transferring of the data is completed.

(3) Stores the compressed image for one page read out from the DRAM, in the HDD.
Deletes the page image in the DRAM after storing of the compressed image in the HDD is completed.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.



Step2

(4) Transfers the image data read out from the HDD to the DRAM.

(5) Converts the compressed image data in the DRAM into the compressed image in compression format supported in each protocol or that supported in the designated file format, then converts into the designated image format.
At this image format conversion, encryption using password, encryption by digital certificate, and signature processing are also executed.

(6) Transfers the converted file to the external device using each protocol.

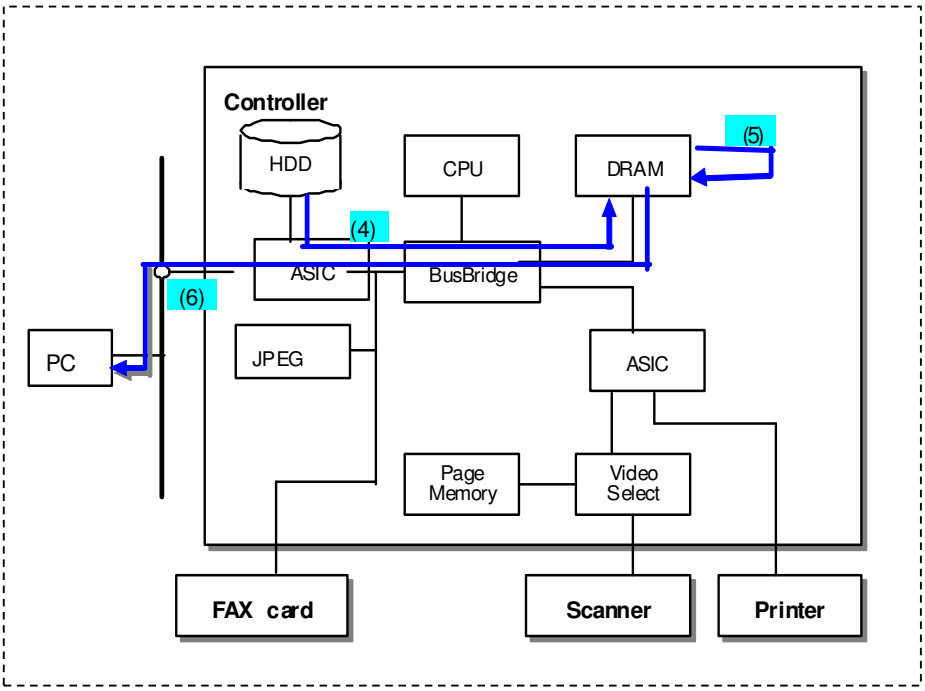
(7) Deletes the document image in the Mailbox and DRAM after transferring of the file is completed.

S/MIME Communication (Signature and Encryption)

In S/MIME communication (signature), signature is added per mail when sending data to the network in SMTP (operation (7) above) based on the certificate information retained in the device.

In S/MIME communication (encryption), encryption is performed per mail when sending data in SMTP (operation (7) above) based on the certificate corresponding to the designated address.

In S/MIME communication, certificate is verified when sending of the data is designated as well as when the data is to be sent. S/MIME communication is conducted only when validity of the certificate is confirmed.



4.5.2 Scan to Mailbox

In scan to Mailbox, image data scanned by the scanner is stored in the Mailbox.

<Operation>

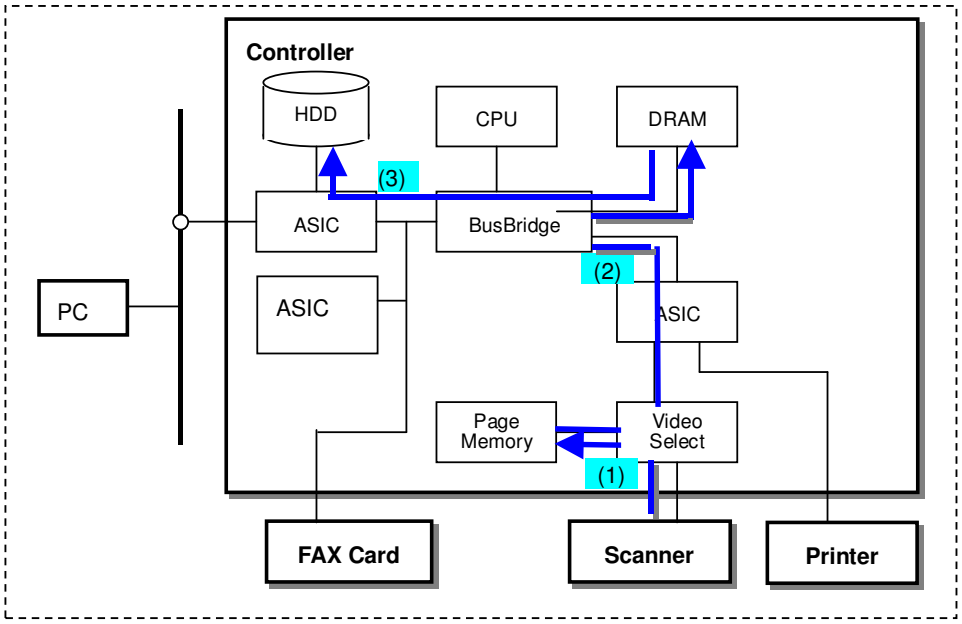
(1) Stores the image data scanned by the scanner in the page memory.

(2) Transfers the image data for one page read out from the memory to the DRAM after compression.
Deletes the image in the page memory after transferring of the data is completed.

(3) Stores the compressed image for one page read out from the DRAM, in the HDD (Mailbox).

(4) Deletes the page image in the DRAM after transferring of the data is completed.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.



4.5.3 Mailbox to PC

In Mailbox to PC, data stored in the Mailbox is transferred to the external device.

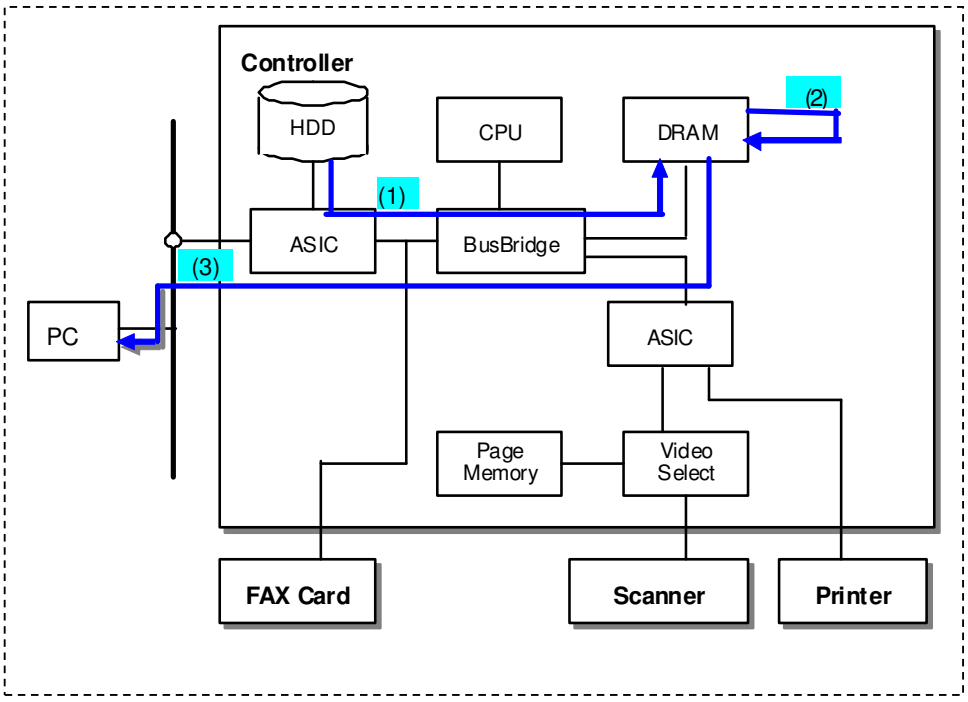
<Operation>

(1) Transfers the image data read out from the Mailbox to the DRAM.

(2) Converts the stored file into the file in compression format supported in each protocol or that supported in the designated file format, then converts into the designated image format.
At this operation, security feature described in section 4.5.1 can also be used.

(3) Transfers the converted file to the external device using each protocol.

(4) Deletes the document image in the Mailbox and DRAM after transferring of the file is completed.



4.5.4 Scan to USB

In Scan to USB service, the image data scanned by the scanner is converted into multipurpose image format (TIFF/JFIF/XDW/PDF/XPS) and transferred directly to the USB memory connected to the USB port on the device.

<Operation>

Step 1

(1) Stores the image data of multiple pages in the HDD as is the same as Step 1 of "4.5.1 Scan to PC Service."

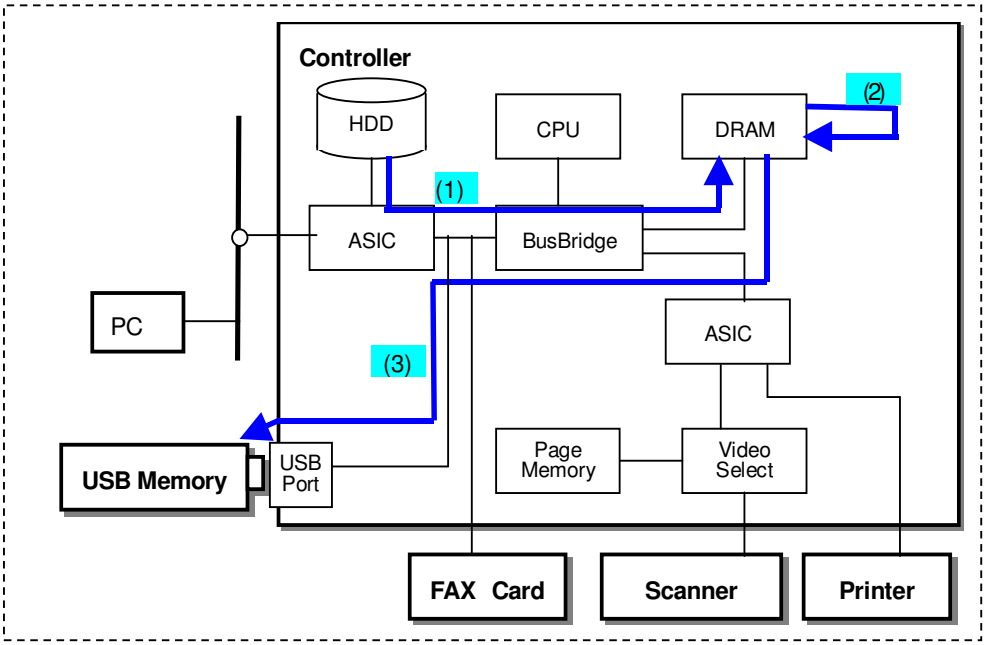
Step 2

(2) Converts the image data into the file format designated by user as is the same as (5) to (6) of Step 2 in "4.5.1 Scan to PC Service."

At this point, the security features (per format) indicated in section 4.5.1 can be used as well.

(3) Transfers the converted file to the USB memory connected to the USB port.

(4) Deletes the document image in the HDD and that in DRAM after the transfer is completed.



4.6 Internet Fax Service

4.6.1 Internet Fax Send

In internet Fax send, B/W binary image data scanned by the scanner is converted into image file format for Internet Fax (TIFF-FX) and sent to the designated mail address as an e-mail (SMTP).
When S/MIME feature is in enabled state, electronic mail can be encrypted using destination's digital certificate and electronic signature on electronic mail can be provided using device's digital certificate, by S/MIME feature.

<Operation>

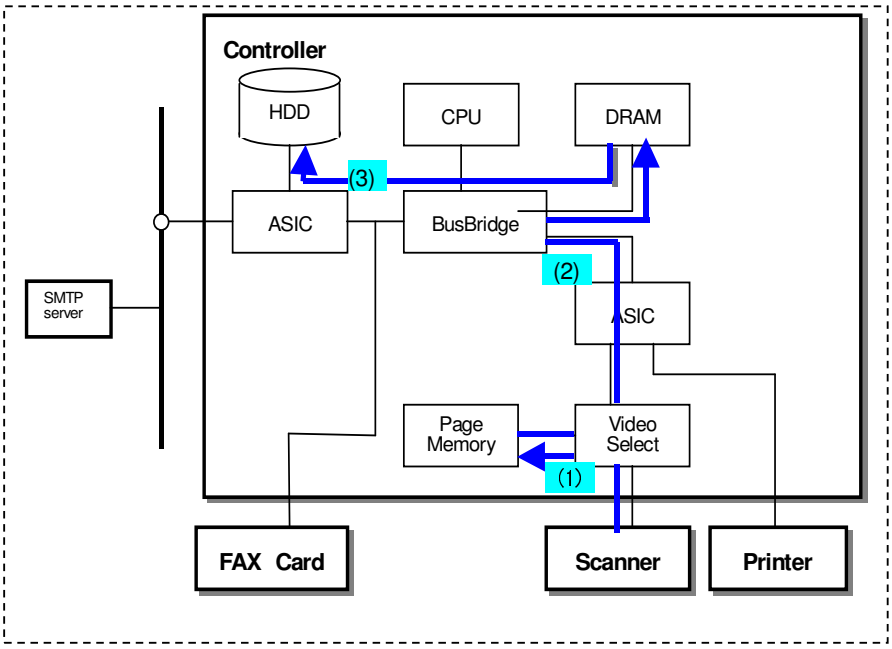
Step1

(1) Stores the image data scanned by the scanner in the page memory.

(2) Compresses the image data for one page read out from the page memory and transfers to the DRAM. Deletes the image in the page memory after transferring of the data is completed.

(3) Stores the compressed image for one page read out from the DRAM, in the HDD. Deletes the page image in the DRAM after storing of the compressed image in the HDD is completed.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.



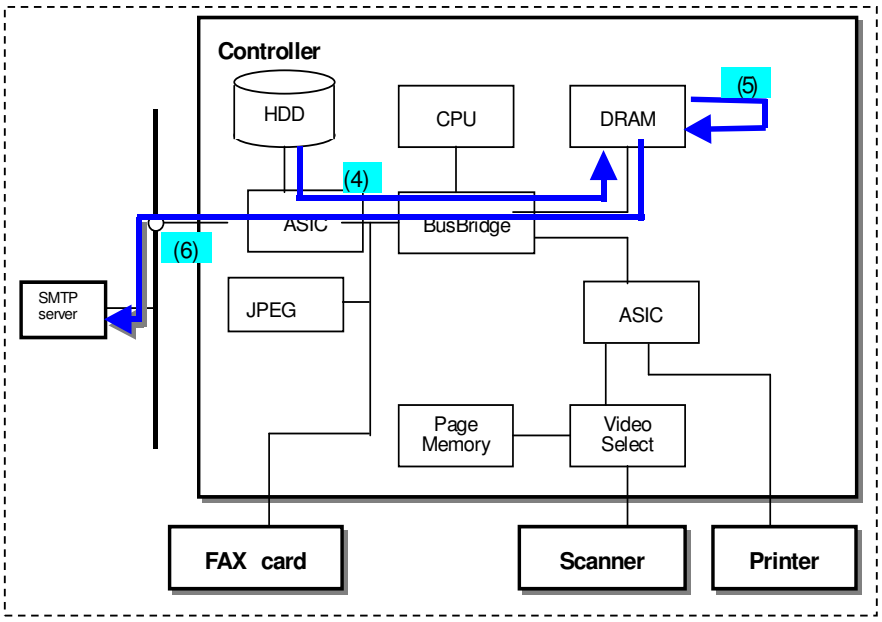
Step2

(4) Transfers the compressed image from HDD to DRAM.

(5) Converts the image format into TIFF-FX format.

(6) Encodes the TIFF-FX file in MIME and sends to the designated mail address as an e-mail (SMTP).
When electronic signature and/or encryption by S/MIME is(are) designated, electronic signature is attached and/or encryption is executed at this stage.
Secret key and digital certificate used for electronic signature and encryption are registered in the certificate repository in HDD. The secret key is always encrypted by device-specific encryption key.

(7) Deletes the information on the document in the HDD and DRAM after sending of the file is completed.



4.6.2 Internet Fax Receive

In internet Fax receive, content of the mail (header, text, attached TIFF file) received in e-mail (SMTP) is output to the printer.
When S/MIME feature is in enabled state and the received mail has S/MIME electronic signature, electronic signature is verified and printed out according to the modes shown below. When the signature is incorrect, the mail is abandoned. When the received mail is an encrypted mail by S/MIME, it will be decoded using the device's secret key.

Reception operation of S/MIME mail with electronic signature

Mode	Operation
Permit reception of unreliable mail	Receives and conducts printing process on non-S/MIME mail and S/MIME mail without signature. Abandons received mail when S/MIME electronic signature is incorrect or its mail address is different from the electronic signature.
Prohibit reception of unreliable mail	Receives and abandons non-S/MIME mail and S/MIME mail without signature. Abandons received mail when S/MIME electronic signature is incorrect or its mail address is different from the electronic signature.

<Operation>

Step1

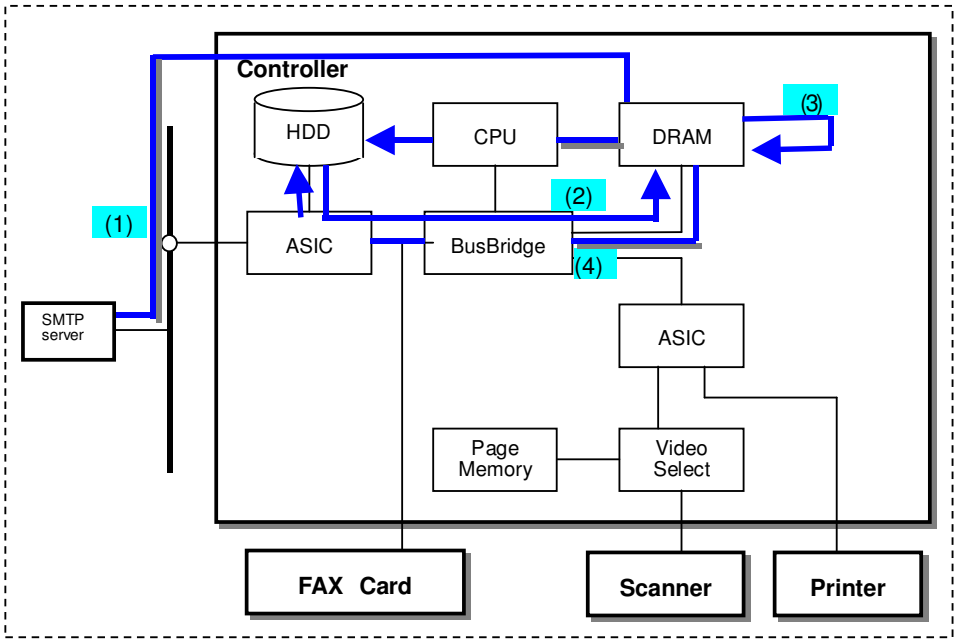
(1) Stores the mail received in e-mail (SMTP/POP), in the HDD.
When the received mail is S/MIME mail, signature on the mail is verified and decoding is conducted at this stage.
Secret key and digital certificate used for electronic signature verification and decoding is registered in the certificate repository in HDD. The secret key is always encrypted by device-specific encryption key.

(2) Transfers the data received in the HDD to the DRAM.

(3) Decodes MIME, separates it into "header and text" and "attached TIFF file", then decomposes each of them.

(4) Compresses each of the decomposed image and stores in the HDD.

(5) Deletes the received document in the HDD and page image in the DRAM.



Step2

See 4.3.4 Fax Print.

4.6.3 Mailbox Receive of Internet Fax (E-Mail to Mailbox)

In Mailbox receive of internet Fax, mail received in e-mail (SMTP/POP) is stored in the Mailbox.

<Operation>

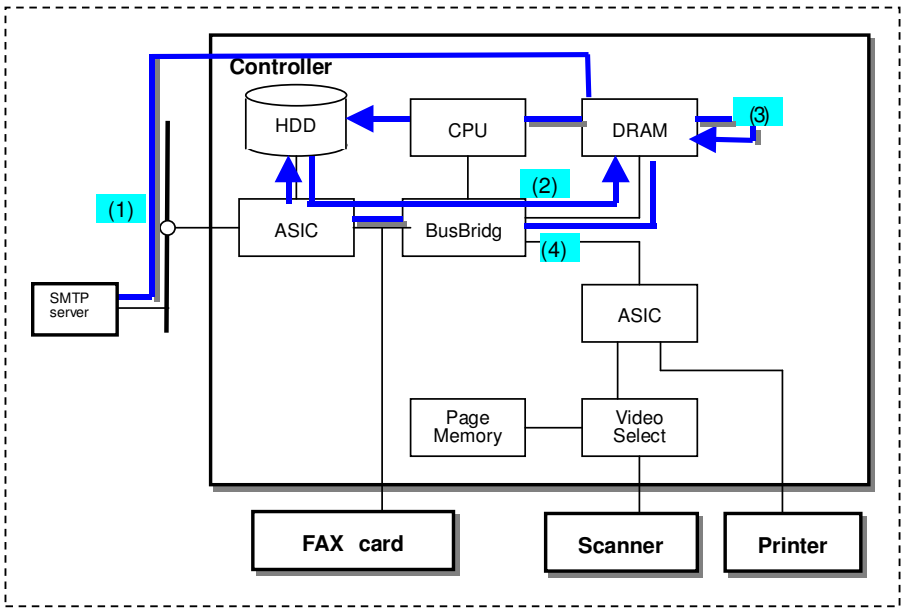
(1) Stores the mail received as e-mail (SMTP/POP), in the HDD.

(2) Transfers the data received in the HDD to the DRAM.

(3) Decodes MIME, separates it into ”header and text” and ”attached TIFF file”, then decomposes each of them.

(4) Compresses each of the decomposed image and stores in the designated Mailbox.

(5) Deletes the received document in the HDD and page image in the DRAM.



4.7 Report Service

4.7.1 Report Print

In report print, the compressed image data of Report is stored in the HDD, then the image data is output to the printer after read out from the HDD.

<Operation>

Step1

(1) Creates PDL to be reported from the system information (NVRAM) and stores in the DRAM.

(2) Reads out the PDL stored in the DRAM.

(3) Decomposes the read-out PDL per page, and writes in the page buffer (DRAM).

(4) Compresses the page buffer per page and transfers to the DRAM.

(5) Reads out the compressed data from the DRAM, then transfers and stores in the HDD.
Deletes the page image in the DRAM after transferring of the data is completed.

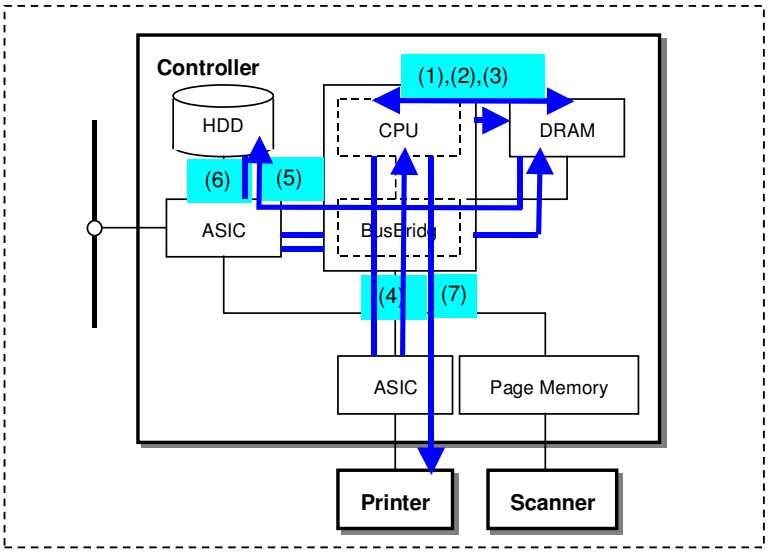
Step2

(6) Reads out the compressed image from the HDD and transfers to the DRAM.

(7) Outputs the compressed image read out from the DRAM to the printer through decompression.

Conducts the operations (6) to (7) for the number of times that equals to the number of pages stored in the HDD.

(8) Deletes the document image in the HDD and page image in the DRAM after printing is completed.



4.7.2 Fax Report Print

This is the operation of Fax Report Print of when PCC Fax Card is installed.

Operation of Fax Report Print of when Fax Card Mini is installed is the same as 4.7.1 Report Print.

In Fax report print, Fax Report is stored in the HDD from the Fax Card, then output to the printer after read out from the HDD.

<Operation>

Step1

(1) Stores the report (compressed data) created by Fax Card, in the DRAM.

(2) Stores the image data read out from the DRAM, in the HDD.
Deletes the page image in the DRAM after the image data is stored.

Step2

(3) Reads out the image data from the HDD and transfer to the DRAM.

(4) Decompresses the image data read out from the DRAM and restores in the DRAM.

(5) Conducts image rotation if necessary.

(6) Compresses the image data read out from the DRAM and restores in the DRAM.

(7) Stores the image data in the HDD, then deletes the page image in the DRAM.

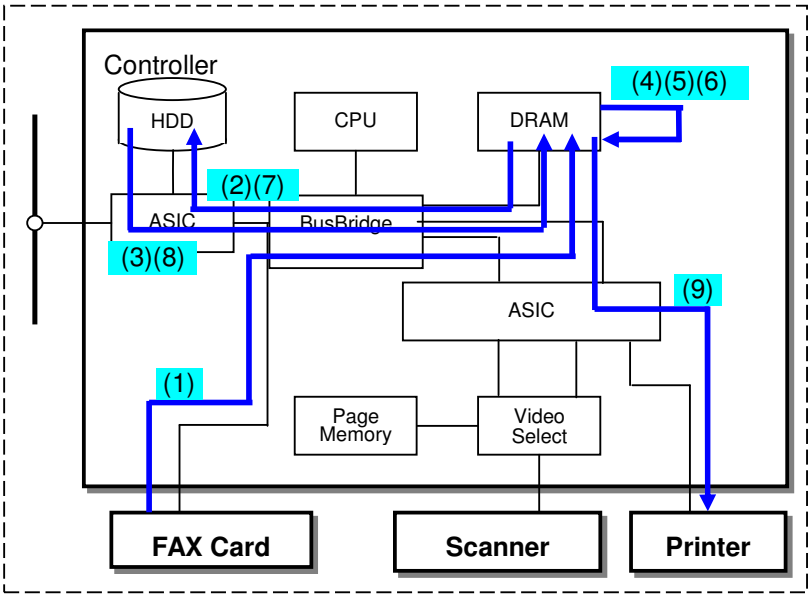
Conducts the operations (3) to (7) for the number of times that equals to the number of Pages stored.

Step3

(8) Reads out the compressed image from the HDD and transfers to the DRAM.

(9) Outputs the compressed image read out from the DRAM to the printer through decompression.
Deletes the page image in the DRAM after the printing for the page is completed.

(10) Deletes the document image in the HDD after all the pages are printed.



Section 5 Protection of Data on the Hard Disk

The product has the following security features that can be used on the data stored in the hard disk.

- Image Overwrite feature
- Data Encryption feature.

5.1 Image Overwrite Feature

Image Overwrite feature is the feature to delete the already used document data that still resides on the Controller hard disk by an overwrite, after the completion of Copy, Print, Scan and Fax operations.

5.1.1 Algorithm

The administrator can select the overwrite algorithm from the following:

"Off"

Image overwrite is not conducted.

"On (once)"

Image overwrite is conducted once with "the data set to all 0".

"On (thrice)"

Image overwrite is conducted thrice with "the random data",
" the random data", and then "the data set to all 0".

5.1.2 Special Behavior

The administrator sets the number of times to overwrite in accordance with the policy. The setting will become valid when the product is started up again.

The Image Overwrite feature is operated when the document data in the Controller hard disk is abandoned after the Copy, Print, Scan or Fax feature is used. (See "Chapter 4: Data Flow" for the abandon timing of the document data.)

The user confirms at the Confirmation screen on the Control Panel whether image Overwrite operation is under way; "In Progress" indication is displayed during the image overwrite operation, and "Standby" indication is displayed when the image overwrite operation is not under way.

If the Image Overwrite does not complete due to causes such as power being cut off during the image overwrite process, the Image Overwrite is performed at the next start up.

5.2 Data Encryption Feature

Data Encryption feature is the feature to encrypt any data to be written to the Controller hard disk before writing the data to the hard disk.

5.2.1 Algorithm

The algorithm used in the product is the 256-bit block encryption that conforms to the AES (Advanced Encryption Standard).
The 256-bit encryption key is automatically created at start up, based on the encryption key set by the administrator and stored in the DRAM. The key is deleted by a power-off, due to the physical characteristics of the DRAM.

5.2.2 Special Behavior

This function is enabled at the time of shipment, but in order to change the encryption key, the following is to be performed.
The menu to set Data Encryption feature is displayed in the setting items for the administrator on the Control Panel.
The administrator sets the Data Encryption feature in accordance with the policy. When setting this feature, the administrator is asked to enter an encryption key and he/she can enter any 12 alphanumeric characters. The setting becomes valid when the product is started up again.
The Data Encryption feature is valid on all the data stored on the Controller hard disk, and the data is encrypted before it is stored in the hard disk. Whenever the data is read out from the hard disk, decryption of the data is performed.

Section 6 Security Audit Log

This feature is enabled when the machine administrator sets “Audit Log Settings.” By enabling this Security Audit Log feature, the following information can be kept track of.
- When, by whom (user), and what was done (task) using the product
- Important events on the product (e.g. error, setting change, user operation, etc.)

Events targeted for audit log are recorded to the NVRAM with timestamps. When the number of events reaches 50, they are stored in the hard disk of the product. Up to 15,000 events can be stored in the hard disk. When the number of events exceeds 15,000, audit log files will be deleted in order of timestamp, and then new events will be recorded.

Access to audit log is possible only when the machine administrator uses the Web browser. Access from the control panel is not possible. When the user accesses the product through Web browser, there is an ”Export as text file” button. By pressing that button, audit logs can be downloaded as tab-delimited text files. When downloading audit log data, SSL/TSL communication must be enabled.

Section 7 APPENDICES

7.1 Appendix A-1 – Supported MIB Objects

The supported version of SNMP protocol is 1 (SNMPv1), 2 (SNMPv2), and 3 (SNMPv3). (Multilingual)
The MIB definition implemented for "SNMP agent" is the subset of IETF MIB and that of XCMI MIB, and is also the subset of the management data defined in the following modules.

<IETF MIB>

- MIB-II (RFC1213, RFC1573)
- Host Resources MIB (RFC1514)
- Printer MIB (RFC1759)
  (Printer MIB v2(RFC3805))
- Printer Finishing MIB(RFC3806)
- Printer Port Monitor MIB(wd-pmpportmib10-20050921.mib)
- snmpFrameworkMIB (RFC3411)
- snmpMPDMIB (RFC3412)
- snmpUsmMIB (RFC3414)
- snmpVacmMIB (RFC3415)

<XCMI MIB(V5.4)>

- Common (02common.txt)
- General Textual Conventions (06gentc.txt)
- General MIB (07gen.txt)
- Host Resources MIB Extensions Textual Conventions(10hosttc.txt)
- Host Resources Extensions MIB(11hostx.txt)
- Printer MIB Extensions Textual Conventions(15prtxtc.txt)
- Printer MIB Extensions(16prtx.txt)
- Document Resources Textual Conventions(21rsrctc.txt)
- Document Resources MIB(22rsrc.txt)
- Job Monitoring MIB Textual Conventions(40jobtc.txt)
- Job Monitoring MIB (41jobmon.txt)
- Simple Job Management Textual Conventions(42jobmtc.txt)
- Simple Job Management MIB(43jobman.txt)
- Communications Configuration MIB Textual Conventions(52conftc.txt)
- Communications Configuration MIB(53config.txt)
- Service Monitoring MIB Textual Conventions(58svctc.txt)
- Service Monitoring MIB(59svcmon.txt)

<FX Standard>

- FX Product Identifier Textual Conventions (f93pidtc.txt)
- fxPropJobMonExtMIB.mib

7.2 Appendix A-2 – Supported SESAMi Service Management Interface

The SSMI (SESAMi Service Management Interface), which provides the following features as the device management interface is supported.

Applicable products:

Xerox WorkCentre 5325/5330/5335

Supported feature	Description
Status/Config Management	Provides the means to obtain and set the information subject to management. To be more precise, the feature to obtain the description on the various setting values and status values of the device (GetDescription), to obtain the attributes (GetAttribute), and to set the attributes (SetAttribute).
Job Management	Provides the means to manage processing jobs and completed jobs. To be more precise, the means to obtain job information (logs) (GetJobList), to control jobs in process (OperateJob), and to obtain job information (logs) including parent-child job relationships (GetJobListEx).
Exclusive Control	A control service used for exclusive access to features provided by SSMI. To be more precise, the feature to start exclusive control by creating context for access (CreateExclusiveContext) and to end exclusive control by releasing context for access (ReleaseExclusiveContext).
Service State Management	Instructs the state transition of the service (device) (OperateService). (e.x. instructs rebooting.)
User Management	Manages users. To be more precise, provides the features to add (AddUser), delete (DeleteUser), obtain (GetUser), and set (SetUser) users managed by the product.
User Information Management	Manages the information associated with users (Service use counter / use restriction, per user). To be more precise, provides the features to obtain (GetUserInformation) and set (SetUserInformation) user information.
Account Management	Manages the Account ID. To be more precise, provides the features to obtain (GetAccountID), set (SetAccountID), and delete (DeleteAccountID) Account ID.
Address Book Management	Manages the Address Book, which contains information such as the speed dials and server addresses. To be more precise, provides the features to add (AddAddress), delete (DeleteAddress), obtain (GetAddress)/, and set (SetAddress) such information.
Job Flow Sheet	Manages the Flow Sheets (i.e. Job Flow Sheets). To be more precise, provides the

Management	features to add (AddJob Flow Sheet), delete (DeleteJob Flow Sheet), obtain (GetJob Flow Sheet), and set (SetJob Flow Sheet) Job Flow Sheets.
Job Flow Sheet Owner Management	Manages the owners of each Flow Sheet (Job Flow Sheet). To be more precise, provides the features to obtain (GetJob Flow SheetOwner) and set (SetJob Flow SheetOwner) the owner of Job Flow Sheet.
Mailbox Management	Manages the Mailboxes. To be more precise, provides the features to add (AddMailbox) and delete (DeleteMailbox) Mailbox, and obtain (GetMailbox) and set (SetMailbox) the Mailbox setting information.
Key Management	Manages the certificates. To be more precise, provides the features to add (AddKey), delete (DeleteKey), obtain (GetKey), and assign (AssignKey) key.
Local Key Management	Generates the self-certificates. To be more precise, provides the features to generate (Generate) self-certificates.
Chain-Link Management	Manages Chain-Link. To be more precise, provides the features to obtain(GetChainLink) and set (SetChainLink) Chain Link.
Job Log Management	Manages the job logs. To be more precise, provides the features to obtain the job log information (GetJobLogInfo) and obtain the job log (GetJobLog).
Accounting Relation Management	Manages the relation between the Account ID and User ID. To be more precise, provides the features to add (AddAccountingRelation), delete (DeleteAccountingRelation), and obtain (GetAccountingRelation) the accounting relations.
Custom Service Management	Provides management features of registering, changing, and deleting custom service scripts, and obtaining list of custom service scripts. To be more precise, provides folder management, script file management, and service management features. [Folder management] Create folder to register custom service script files (CreateCsvFolder) / Obtain list of names of folders to register custom service scripts (ListCsvFolder) / Delete folder to register custom service script files (DeleteCsvFolder) [Script file management] Register custom service script to folder (StorCsvFiles) / Delete custom service script from folder (DeleteCsvFiles) [Service management] Register folder in which custom service script is stored to custom service (AddCsv) / Change content of registered items in custom service (SetCsv) / Obtain list of custom services (ListCsv) / Delete registered items from custom service (DeleteCsv)

7.3 Appendix B – Networking Protocol RFC's and Standards

See Appendix A for details of RFC related to SNMP/MIB.

ID	Title
IEEE Ethernet 802.3	Ethernet
RFC1035	Domain names – implementation and specification
RFC1042	Standard for the transmission of IP datagrams over IEEE 802 networks
RFC1071	Computing the Internet checksum
RFC1122	Requirements for Internet Hosts – Communication Layers
RFC1123	Requirements for Internet Hosts – Application and Support
RFC1191	Path MTU discovery
RFC1321	The MD5 Message-Digest Algorithm
RFC1323	TCP Extensions for High Performance
RFC1518	An Architecture for IP Address Allocation with CIDR
RFC1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC1624	Computation of the Internet Checksum via Incremental Update
RFC1639	FTP Operation Over Big Address Records (FOOBAR)
RFC1831	RPC: Remote Procedure Call Protocol Specification Version 2
RFC1981	Path MTU Discovery for IP version 6
RFC2001	TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms
RFC2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC2113	IP Router Alert Option
RFC2131	Dynamic Host Configuration Protocol
RFC2132	DHCP Options and BOOTP Vendor Extensions
RFC2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC2236	Internet Group Management Protocol, Version 2
RFC2292	Advanced Sockets API for IPv6
RFC2373	IPVersion 6 Addressing Architecture
RFC2374	An IPv6 Aggregatable Global Unicast Address Format
RFC2375	IPv6 Multicast Address Assignments
RFC2428	FTP Extensions for IPv6 and NATs

RFC2460	Internet Protocol, Version 6 (IPv6) Specification
RFC2461	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462	IPv6 Stateless Address Autoconfiguration
RFC2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC2464	Transmission of IPv6 Packets over Ethernet Networks
RFC2526	Reserved IPv6 Subnet Anycast Addresses
RFC2553	Basic Socket Interface Extensions for IPv6
RFC2581	TCP Congestion Control
RFC2710	Multicast Listener Discovery (MLD) for IPv6
RFC2711	IPv6 Router Alert Option
RFC3363	Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
RFC3596	DNS Extensions to Support IP Version 6
RFC1157	Simple Network Management Protocol (SNMP)
RFC1420	SNMP over IPX
RFC1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1514	Host Resources MIB
RFC1759	Printer MIB
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1001	PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS
RFC1002	PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS
RFC1945	Hypertext Transfer Protocol -- HTTP/1.0
RFC2616	Hypertext Transfer Protocol -- HTTP/1.1
RFC2617	HTTP Authentication: Basic and Digest Access Authentication
RFC1179	Line printer daemon protocol
RFC959	File Transfer Protocol
RFC1510	The Kerberos Network Authentication Service (V5)
RFC2246	The TLS Protocol Version 1.0
RFC821	Simple Mail Transfer Protocol
RFC822	STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES
RFC1939	Post Office Protocol - Version 3

RFC2165	Service Location Protocol (SLP)
RFC2251	Lightweight Directory Access Protocol (v3)
RFC2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC2910	Internet Printing Protocol/1.1: Encoding and Transport
RFC2911	Internet Printing Protocol/1.1: Model and Semantics
RFC2518	HTTP Extensions for Distributed Authoring -- WEBDAV
RFC2401	Security Architecture for the Internet Protocol
RFC2402	IP Authentication Header
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409	The Internet Key Exchange (IKE)
RFC2412	The OAKLEY Key Determination Protocol
RFC1828	IP Authentication Using Keyed MD5
RFC1829	The ESP DES-CBC Transform
RFC2085	HMAC-MD5 IP Authentication with Replay Prevention
RFC2403	The Use of HMAC-MD5 within ESP and AH
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2410	The NULL Encryption Algorithm and Its Use With IPSec
RFC2451	The ESP CBC-Mode Cipher Algorithms
RFC2631	Diffie-Hellman Key Agreement Method
RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPSec
RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec
RFC3686	Using Advanced Encryption Standard (AES) Counter Mode With IPSec Encapsulating Security Payload (ESP)

7.4 Appendix C – Connector Layouts

The connectors shown below are set on the back of the product and the user interface.